T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİBER SALDIRI ALTINDAKİ VERİ MERKEZLERİNDE YER ALAN SANAL MAKİNELERİN OPTİK AĞ ALTYAPISI ÜZERİNDEN TAHLİYESİ

YÜKSEK LİSANS TEZİ

Emre KARAKOÇ

Enstitü Anabilim Dalı	**:**	**BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Yrd. Doç. Dr. Ferhat DİKBIYIK**

Haziran 2016

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİBER SALDIRI ALTINDAKİ VERİ MERKEZLERİNDE YER ALAN SANAL MAKİNELERİN OPTİK AĞ ALTYAPISI ÜZERİNDEN TAHLİYESİ

YÜKSEK LİSANS TEZİ

Emre KARAKOÇ

Enstitü Anabilim Dalı	:	**BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ**
Tez Danışmanı	:	**Yrd. Doç. Dr. Ferhat DİKBIYIK**

Bu tez 27.06.2016 tarihinde aşağıdaki jüri tarafından oybirliği / ~~oyçokluğu~~ ile kabul edilmiştir.

Yrd. Doç. Dr. Ferhat DİKBIYIK	**Prof. Dr. Celal ÇEKEN**	**Doç. Dr. Ayşegül GENÇATA YAYIMLI**
Jüri Başkanı	**Üye**	**Üye**

Haziran 2016

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.

İmza

Emre KARAKOÇ

27.06.2015

TEŞEKKÜR

Yüksek Lisans eğitimim boyunca, tez konumu belirlemede ve tez çalışmamın her aşamasında tavsiye ve yönlendirmeleri ile bana ışık tutan değerli danışmanım Yrd. Doç. Dr. Ferhat DİKBIYIK'a ve benden desteklerini hiçbir zaman esirgemeyen eşime ve aileme manevi desteklerinden dolayı teşekkür ederim.

Bu çalışma TUBİTAK 3001 – Başlangıç Ar-Ge Projeleri Destekleme Programı tarafından desteklenmiştir. Proje Numarası: 116E011.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

APON	: ATM Passive Optical Network
BPON	: Broadband Passive Optical Network
CaaS	: Cloud as a Service
GPON	: Gigabit Passive Optical Network
LMAS	: Live Migration Acceleration System
NIST	: National Institute of Standards and Technology
IaaS	: Infrastructure as a Service
ILP	: Integer Linear Programming
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
PaaS	: Platform as a Service
PON	: Passive Optical Network
SOME	: Siber Olaylara Müdahale Ekibi
SaaS	: Software as a Service
WAN	: Wide Area Network

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Siber Güvenlik; Bulut Bilişim, Sanal Makine Migrasyonu, Optik Veri Merkezi Ağı.

Sanallaştırma teknolojileri son yıllarda hızla yaygınlaşmaktadır. Sanallaştırma teknolojisinin kullanıldığı veri merkezlerinde önemli problemlerden biri veri merkezlerine yapılan siber saldırılardır. Bir saldırı anında sadece bir veya birkaç sanal makine değil bulut sistemi içindeki tüm veri merkezlerinde bulunan sanal makineler tehlike altındadır. Bu saldırılar sonucunda veri kayıpları ciddi oranda artmaktadır. Ufak bir bilgi kaybı veya bilgi çalınması durumunda hizmet alan ilgili şirketlerde büyük mali zararlar veya prestij kayıpları meydana gelmektedir. Ayrıca güncel güvenlik teknikleri siber saldırılara karşı birtakım önlemler almasına rağmen bu saldırılar sonucunda çoğu zaman verilerde hasar ve çalıntı olmakta, hatta çoğu bulut bilişim hizmeti uzun süre hizmet veremeyecek duruma gelmektedir.

Bu çalışmada, bu problemi önlemek amacıyla optik ağ üzerinden birbirlerine bağlı bulunan veri merkezlerinin oluşturduğu bir bulut sistemine yapılacak olası bir siber saldırıda zararlı yazılım bulaşmış makinelerin karantinaya alınarak temizlenmesi ve zararlı yazılımların aynı optik ağdaki diğer makinelere bulaşmaması için bir güvenlik modelinin oluşturulması ele alınmıştır.

Saldırı tespit mekanizmalarının verdiği erken uyarılar dikkate alınarak, zararlı yazılım bulaşma ihtimali olan sanal makinelerin çok kısa süre içerisinde başka bir lokasyona taşınması (migration) sağlanarak siber saldırıların verebileceği hasar boyutu minimize edilmiştir.

RAPID EVACUATION OF VIRTUAL MACHINES ON A DATACENTER UNDER CYBER ATTACK OVER OPTICAL INFRASTRUCTURE

SUMMARY

Keywords: Cyber Security, Cloud Computing, Virtual Machine Migration, Optical Datacenter Network

Virtualization technologies are becoming increasingly common in recent years. One of the major problems in institutions and organizations using virtualization technology is cyber attack to servers. In case of an attack, not only one or a few virtual machines are under the risk, but all datacenters in the cloud face the risk of cyber attack. These attacks result in data loss is increasing dramatically. Users that take these services keep many critical and important data, programs, or systems in these cloud computing environments. In case of data loss or stolen data, corporations served experience major monetary loss and prestige loss. Besides, even though up-to-date security techniques take countermeasures against cyber attacks, damages on data and systems can still be occurred in cloud systems and many cloud computing systems may be unavailable for a long period of time In this case, service providers have to pay huge amounts to their customers due to security contracts made with their users.

In this study, it's discussed that is development of a security model for cleaning virtual machines by taking them to quarantine centers in case of a cyber attack to a cloud system formed by datacenters connected over an optical network and for avoiding dissemination of attack to other datacenters on the same optical network.

This model helps to minimized size of the damage due to cyber attack by rapidly migrating virtual machines under the risk of malware infection to other locations by taking the warnings provided by intrusion detection mechanisms into consideration.

BÖLÜM 1. GİRİŞ

Bu çalışmanın amacı, optik ağ üzerinden birbirlerine bağlı bulunan veri merkezlerinin oluşturduğu bir bulut sistemine yapılacak olası bir siber saldırıda zararlı yazılımların aynı optik ağdaki diğer makinelere bulaşmaması için bir güvenlik modeli oluşturmaktır. Bu modelde, zararlı yazılımın bulaştığı kesin olan sanal makineler ise taşınmadan bulundukları veri merkezinde karantinaya alınabilir. Burada zaman önemli bir faktör olduğundan zararlı yazılımın bulaşıp bulaşmadığı kesin olmayan şüpheli sanal makinelerin ise saldırı altındaki veri merkezlerinde tutuldukları her dakika onlara da zararlı yazılımın bulaşması riskini arttırabilir. Onların da belirli kontrollerin yapılabileceği zararlı yazılım tespit ve koruma merkezlerine aktarılması ve kontrollerin o merkezlerde yapılması daha güvenli olacaktır. Diğer taraftan saldırı tespit mekanizmalarının verdiği uyarılar dikkate alınarak, zararlı yazılım bulaşma ihtimali olmayan güvenli sanal makinelerin çok kısa süre içerisinde başka bir lokasyona taşınması sağlanıp, siber saldırıların verebileceği hasar boyutu minimize edilebilir. Bu doğrultuda üretilecek çözüm, saldırının zararlarını minimuma indirmeyi hedeflediğinden bu çalışma bir optimizasyon problemi olarak düşünülebilir.

Son yıllarda internet sayesinde hemen hemen her türlü bilgisayar, mobil, TV, tablet vb. cihazlar birbirlerine bağlanabilmekte ve bulut bilişim hizmetleri sunan servis sağlayıcılar sayesinde etkileşime geçerek web servisleri üzerinden kaynak paylaşımı yapabilmektedirler. Günümüzde, ülkemizin de içerisinde olduğu gerek gelişmiş gerek gelişmekte olan ülkelerde kişisel ve kurumsal verilerin izole depolama alanları yerine genel (public) veya özel (private) bulutlarda saklandığı ve işlendiği görülmektedir. Bulut bilişim teknolojileri kişileri ve kurumları gerçek makinelerin bakımı, güncellemesi, vb. sıkıntılardan kurtararak sanal makineler kullanmayı cazip hale getirmiştir. Genellikle optik ağ omurgası üzerinden birbirlerine bağlı olan veri

merkezlerinden oluşan bulutlarda milyonlarca kişinin ve kurumun bilgileri veri havuzlarında toplanmaktadır. Bulut bilişim hizmeti sunan şirketler, veri merkezlerini birbirine bağlayan optik altyapıyı kiralayabildikleri gibi Google, Amazon, Facebook gibi şirketlerde olduğu gibi kendi optik ağ altyapılarını da geliştirebilirler. Bu bağlamda veri merkezleri gün geçtikçe ürün olmaktan daha çok servis hizmetleri olma yolunda değişim göstermektedir ve bu hizmetlerin hem maddi olarak ucuzlaması hem de erişim ve kullanım kolaylıkları sebebiyle çoğu kullanıcı tarafından tercih sebebi olmaktadır. Hizmet alan bu kullanıcılar kendilerine ait birçok kritik ve önem arz eden bilgileri, programları veya sistemlerini bu bulut bilişim ortamında saklamaktadırlar. Ufak bir bilgi kaybı veya bilgi çalınması durumunda hizmet alan ilgili şirketlerde büyük mali zararlar ve prestij kayıpları meydana gelmektedir. Ayrıca güncel güvenlik teknikleri siber saldırılara karşı birtakım önlemler almasına rağmen bu saldırılar sonucunda çoğu zaman verilerde hasar veya çalıntı olmakta hatta çoğu bulut bilişim hizmeti uzun süre hizmet veremeyecek duruma gelmektedir. Bu durumda hizmet sağlayıcıları, kullanıcılarıyla yaptıkları garanti sözleşmeleri sebebiyle kullanıcılarına yüksel bedeller ödemek durumunda kalmaktadırlar. Ancak bir saldırı anında sadece bir veya birkaç sanal makine değil bulut sistemi içindeki tüm veri merkezlerinde bulunan sanal makineler tehlike altındadır.

Bilgisayar ağlarının ve internetin yaygınlaşması ile birlikte ortaya çıkan siber saldırı kavramı gün geçtikçe toplumlara, devletlere ve kurumlara verdiği zararlar küçümsenmeyecek kadar arttı. Özellikle son yıllarda ortaya çıkan siber savaşlar, soğuk savaş döneminin yerini aldığını söyleyebiliriz. Dünyada siber saldırıların toplam maliyeti yıllık 388 milyar dolar olarak tahmin edilmektedir [1]. Devletlerin siyasi çıkar ilişkilerine kadar uzanan bu siber savaş olgusu nükleer güvenlik sistemlerinden, enerji santrallerine ve birçok devlet teşkilatların veri merkezlerine kadar etki edebilmektedir. 2007 yılında Estonya hükümetine ve medyasına, 2008 yılında ise Gürcistan'a yönelik bir siber saldırı gerçekleştirilmiştir [1]. 2010 yılında da İran'ın nükleer programına yönelik ise Stuxnet adlı virüs ile bir saldırı gerçekleştirildiği bilinmektedir. Siber savaşlar, ülkelerin siber güvenlik planlarında yer etmeye başlamıştır. Devletler, siber altyapı teknolojilerini tesis etmeye

yönelmişlerdir. ABD, 2009 yılında Siber Savaş Komutanlığı'nı, Çin ise 2050 yılına kadar teknolojik alanda elektronik imparatorluğunu kurmayı hedeflemektedir [1]. Türkiye'de ise 2011 yılında Ulusal Siber Güvenlik Strateji Belgesi Çalıştayı düzenlendiği bilinmektedir [1]. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Türkiye'ye yönelik siber saldırılara karşı SOME (Siber Olaylara Müdahale Ekibi) ile mücadele edileceğini belirtti [1]. Bu amaçla 5 sektörel olmak üzere toplamda 367 kurumsal SOME kurulduğu bakanlık tarafından belirtilmiştir [1]. 2013'de kurulan Ulusal Siber Olaylara Müdahale Merkezi (USOM) sayesinde ise 20 bine yakın "siber tehdit" tespit edildiği ve yaklaşık 300 "zararlı yazılım" ile 5 milyondan fazla "bulaşma girişimi"nin saptandığı belirtildi [1].

Gerçekleştirdiğimiz bu çalışmaya ilişkin literatürde benzer çalışmalar da yer almaktadır. Bunlardan en önemlisi afet anında veri merkezlerinden verilerin tahliyesi üzerine bir çalışma ortaya koymuştur. Bu çalışmada öngörülebilir bir afet sırasında verilerin diğer merkezlere nasıl taşınacağı araştırılmıştır [2]. Bizim çalışmamızın özgün tarafı ise bu tahliye işlemlerini en güncel migrasyon yöntemleri ile gerçekleştirerek siber saldırılara karşı kullanmak olmuştur. Bir diğer çalışmada ise uçuş endüstrisinde kullanılan "kara kutu" teknolojisinden esinlenilmiştir [3]. Çoğu deprem, yangın gibi afet sonrasında bölgede büyük hasarlar meydana geldiğinden veri merkezlerinin de bu afetten etkilenebileceği öngörülmüştür. Dolayısıyla, ağ sensör düğümlerinin afet esnasında hayatta kalma süre zaman aralığını referans alarak, hayati önem arz eden verilerin güvenli bölgeye aktarılması ile ilgili bir çalışma yapılmıştır. Bu iki çalışmada sadece verinin taşınması üzerine durulmuştur. Sanal makinelerin tahliyesi üzerine yoğunlaşmamışlardır. Ayrıca siber saldırıdan ziyade doğal afetler üzerine geliştirilmiş modelleri kapsamaktadırlar.

Yine afet ve veri merkezleri ile ilgili bir başka çalışmada sensör ağlarıyla birlikte afet verilerinin toplanması, afet anında hasar tespiti ve verilerin acil operasyon merkezine iletimini öngören bir çalışma yapmışlardır [4]. Bu çalışmada sensör ağlarının, önceden binalara yerleştirilmiş cihazlar sayesinde moloz altında kalmış insanların koşullarını ve konumlarını tespit edebileceği ve verileri toplayabileceği bir model önermişlerdir. Diğer taraftan afet bölgelerinde ki sensör ağları sayesinde oluşabilecek

zararı ve ziyanı tespit edebileceklerini belirtmişlerdir. Ayrıca çok sayıdaki düğümden verileri hızlı bir şekilde nasıl toplayacaklarını gösteren ve sensör ağlarını birleştiren melez bir ağ şeması tanıtmışlardır.

Siber saldırının içeriden fiziksel saldırı olarak referans alındığı bir çalışmada saldırı sonucu bir saldırı tespit sistemi kurgulamış ve bu sisteme fiziksel olarak saldırı niteliği taşıyabilecek parametreler tanımlamıştır [5]. Bu parametreler ile oluşabilecek saldırılar kamera, sensör ve insan vb. desteği sayesinde erken tespiti öngörülmüştür. Bu çalışmada ise bir saldırı tespit sistemi kurmak yerine saldırı tespit sistemleri ile ortak çalışabilecek bir tahliye sistemi üzerinde durmaktayız

Sanal makinelerin veri merkezinin iskeleti olduklarından dolayı birincil hedef olduklarını istatistiksel olarak iddia eden bir diğer çalışmada, zararlı bir yazılım veya saldırı sonucunda oluşabilecek zararları engellemek amaçlı kurban bilgisayarı uzak erişim imkanı olan başka bir bilgisayara taşınabilirliği ele alınmıştır [6]. Ayrıca bu çalışmada 1 milyon kod satırını geçen hypervisor da kod açığının bulunmamasının çok zor olduğu belirtilmiştir. Bu sebeple saldırılara açık olan böyle bir sistemin tüm açıklarının kapatılsa bile uzun bir süre alacağı dile getirilmiştir. Tahliye konusunu inceleyen çalışmalar daha çok içeriklerin ve verilerin taşınması üzerinde dururken, sanal makinelerin taşınması konusuna odaklanmamışlardır. Fakat önceki çalışmaların da gösterdiği gibi siber saldırılarda sanal makineler, büyük tehdit altındadırlar.

Sanal makinelerin optik ağ altyapısı üzerinden tahliyesi, güncel sanal makine migrasyon yöntemleri ile yapılabilir. Bu yöntemler sayesinde hem hızlı hem de hatasız taşıma imkânı sağlanacaktır. Diğer taraftan migrasyonun gerekliliği, verimliliği ve performansı üzerine yapılan literatür taramasında birçok çalışma yapıldığı görülmüştür. Bunlardan yapılan bir çalışmada, VMWare Vmotion ve Citrix XenMotion adlı iki migrasyon ürününden bahsetmiş ve bunlar arasında bellek tahsisleri, veri transfer protokol ve migrasyon süreleri ile alakalı performans karşılaştırması yapılmıştır [7]. Bu karşılaştırmaya göre belli ağlarda VMotion performansının XenMotion'a göre daha iyi olduğunu belirtmişlerdir. Ayrıca migrasyon teknikleri de her geçen gün geliştirilerek sorunsuz sanal migrasyonlar

sağlanmaktadır. Bunlardan birisi de sanal makinelerin Hypervisor'u değiştirmeye gerek kalmadan XenMotion ve VMotion gibi migrasyon tekniklerine uyarlanabilir bir sistem LMAS(Live Migration Acceleration System)'ın geliştirilmesidir [8].

Bulut sağlayıcıların birçok nedenden dolayı başka bulut sağlayıcılarla ortak olabileceklerini vurgulanan başka bir çalışmada ise herhangi bir saldırı olmasa bile disk yetersizliklerinde sistem hatalarında, güç politikalarının iyileştirilmesinde veya yüksek kullanıcı istek sonucu oluşabilecek bellek taşmalarında bu durumun gerekliliğini dile getirilmiştir [9]. Kiralama usulü ile veri merkezi sağlayıcıların da birbirleriyle karşılıklı olarak sistemlerini kullanabilecekleri iddia edilmiştir. Rich Miller tarafından kaleme alınan bir yazıda Amazon'un kapasite sorunu nedeniyle 10 veri merkezini başka bir veri merkezine taşıma ihtiyacı duyduğunu ve bunun için taşınacak veri merkezleri için sanal taşıma yapıldığını vurgulamıştır [10]. Tüm bu araştırmalar dâhilinde sonuç olarak migrasyon teknolojisinin bir yenilik olmasından çok bir gereklilik olduğunu söyleyebiliriz.

Bu çalışmada Bölüm 2'de veri merkezleri ile ilgili genel bilgiler verilmiş ve veri merkezlerinde olması gereken uluslararası standartlar anlatılmıştır. Diğer taraftan veri merkezlerinin altyapısını oluşturduğu bulut bilişim teknolojilerindeki servis modelleri ve servis hizmetleri ele alınmıştır. Ayrıca aynı bölümde veri merkezlerinin temel yapı taşını oluşturan sanal makineler ve sanal makine migrasyon yöntemleri anlatılmıştır. Bölüm 3'de problemin tanımı yapılmış ve daha sonra sistemin genel özellikleri anlatılmıştır. Yine bu bölümde problemin çözümü için sistemin matematiksel modellemesi yapılarak, formülasyonun çalışması ile ilgili örnek bir senaryo verilmiştir. Bu model lineer programlamada çözümü yapılacak amaç fonksiyonunu ve kısıtları içermektedir. Ayrıca bu matematiksel model üzerinden açıklayıcı sayısal örnekler verilmiştir. Verilen örneklerden bir tanesi bu bölümde ayrıntılı olarak açıklanmıştır. Bölüm 4'de elde edilen tüm sonuçlar değerlendirilerek sistemin maliyet ve başarım oranları analiz edilmiştir. Bölüm 5'de ise verilen örneklerin analizi yapılmıştır. Ayrıca yine bu bölümde gelecek çalışmalar ve bu çalışmanın getirileri ile ilgili hedefler açıklanmıştır.

BÖLÜM 2. GENEL BİLGİLER

2.1. Veri Merkezlerinin Genel Özellikleri

Veri merkezleri, genel olarak sunucu, depolama cihazı, ağ cihazı ve telekom araçlarının birlikte güvenli bir şekilde çalışmalarının sağlandığı, saklandığı, korunduğu ve bununla birlikte hizmet sağlayıcıların kullanıcılara kesintisiz ve hızlı bir şekilde hizmet verebilmesi için güçlü bir iklimlendirmeye sahip olan gerekli teknik ağ alt yapısının oluşturulduğu mekânlar olarak tanımlanabilir [11]. Başka bir deyişle kurumların veya kişilerin bilgilerinin saklama ve yedekleme, barındırma, elektronik posta, alan adı hizmetleri, donanım, yazılım, siber güvenlik, sistem entegrasyonu ve uzak bağlantı kurulumu hizmetleri veren büyük altyapılardır. Bilgi sistemlerinin merkezi olan standartlara uygun bir veri merkezi; yeni teknolojilerle donanmış, farklı veri tiplerini barındıran, yüksek derecede erişebilirlik sağlayan ve verilerin tipleri için barındırma hizmeti sağlayan tesislerdir [12].

Son yıllarda Bulut Bilişimin yaygınlaşması ile özel ve kamu kurumları veri merkezlerindeki sakladıkları bilgilerin yüksek seviyede güvenlik ve standartlara uygunluğun sağlanmasını önemsemektedirler. Kurumlar açısından BT altyapılarının güvenli ve sağlam olmasını istemelerindeki en temel sebep güvenlik konusunda yaşanan zafiyetler ve kurumların kontrolü elinde bulundurma istekleri olup bunun temelinde ise bilginin üçüncü kişilerin eline geçmesi endişesidir [11]. Güvenlik zafiyetlerinin gün geçtikçe artması ile kurumların barındırma hizmetlerinin ve uygulamalarının dışarıdan alımına ivme kazandırmıştır. Bununla beraber teknolojideki yeni gelişmeler; farklı kurumlarda ve/veya kurumlara bağlı birimlerde ayrı ayrı bulunan ve işletilen sunucuların, kullanıcı bilgisayarlarının, iş istasyonlarının, haberleşme servislerinin ve bilgi teknolojileri personeli gibi bilgi teknolojileri altyapısına ilişkin tüm hizmetlerin güvenli şekilde birleştirilmesine olanak sağlamaktadır. Bu sayede sistemler ve verilen hizmetler daha verimli ve

güvenli kullanılarak yazılım-donanım altyapısı, personel ve işletme giderleri azaltılarak maliyetler düşmektedir.

Şekil 2.1. Bir Veri Merkezi ([13]'den alınmıştır).

Microsoft'un ABD'de kurduğu bir veri çiftliği 46.000 metre kare alanda, 500 milyon ABD Doları maliyetle kurulmuş ve yaklaşık 400.000 sunucu bulundurmaktadır. Bunun gibi yaklaşık ABD'de 7000'i geçkin veri merkezinin bulunduğu belirtilmektedir.

2.1.1. Veri merkezi türleri

Veri Merkezi türleri genel olarak dört kısımda ele alınabilir [14];

1. Genel Bulut Sağlayıcıları (Amazon, Google) [4]
2. Bilimsel Bilgi İşlem Merkezleri (Ulusal Laboratuvarlar)
3. Sunucu Barındırma Hizmet Merkezleri
4. Kurum İçi Veri Merkezleri

2.1.2. Veri merkezi standartları

Veri merkezlerindeki verilerin işlenme ve saklanma tipine veya önem derecesine göre veri merkezi altyapı sistemleri değişmektedir. Bu bağlamda genel olarak ifade etmek istersek veri merkezlerini veri iletişim cihazları, güç kaynakları ve bu cihazların yedekleri ile veri merkezindeki sistemlerin soğutulması için kullanılan

iklimlendirme sistemleri, yangın söndürme sistemleri ve dış ortamdan gelebilecek tehlikelere karşı verinin güvenlik derecesine göre güvenlik sistemlerini bulundururlar [15]. Standartta veri merkezleri için 4 farklı sınıflandırma belirlenmiş olup, sınıflarla ilgili özet bilgi aşağıda verilmiştir [16].

Tier 1 Seviyesi;

- Küçük işletmelere hizmet veren veri merkezleridir [16].
- Bilgisayar sistemleri, elektrik, mekanik tesisat yedeksizdir [16].
- Genel olarak 10 dakikadan daha fazla bir enerji kesintisine bir önlemi yoktur [16].
- Tahmini %99,676 kullanılabilirlik sunmaktadır [16].

Tier 2 Seviyesi;

- Enerji ve soğutma sistemlerinde kısmen yedeklik içerir [16].
- Jeneratör kullanarak 24 saatlik bir enerji kesintisine dayanabilmektedir [16].
- Tahmini %99,741 kullanılabilirlik sunmaktadır [16].

Tier 3 Seviyesi;

- Yedek elektrik şebekesi içerir [16].
- Yedek enerji ve soğutma sistemleri içerir [16].
- Yedek hizmet sağlayıcıları içerir [16].
- 72 saatlik bir kesintiye karşı dayanabilir [16].
- Tahmini %99,982 kullanılabilirlik sunmaktadır [16].
- Türkiye'de Türk Telekom'un veri merkezi bu standartlara uygun olarak tasarlanmıştır.

Tier 4 seviyesi;

- Bütün Tier 3 kriterleri sağlanır [16].
- Ek olarak 96 saatlik kesintiye dayanabilir [16].
- 7/24 çalışan bir personel ekibi mevcuttur [16].
- Yer seçiminde çok sıkı davranılır, yüksek güvenlik önlemleri alınmıştır [16].

%99,982 ile %99,995 arasındaki fark %0,013 çok küçük bir değer gibi gözükse de uygulama değerlerine göre önem arz etmektedir [16]. Bir yıllık örneğin 525.600 dakikalık bir süreyi dikkate alırsak, Tier 3 seviye 94,608 dakika kullanım dışı olurken, Tier 4 seviye 26,28 dakika kullanım dışı olacak böylece Tier 4 seviye Tier3'den 68,328 dakika daha fazla serviste olacaktır. Bu gibi hassas değerlerin ön planda olduğu veri merkezlerinde fiziksel altyapının güçlü olmasının yanı sıra siber güvenliğinin de sağlam olması gerekmektedir. Herhangi bir siber saldırı sonucunda özellikle banka gibi yüksek önem arz eden kurumlarda yapılan anlık işlemlerde veri merkezinin servis dışı kalması kurum için büyük bir finansal kayıplara sebep olabilir.

Tablo 2.1. Uptime Institute Veri Merkezi Standartları ([15]'den alınmıştır).

Tier	Jeneratör	UPS	Güç Beslemesi	Klima	Kullanılabilirlik	Kesinti Süresi
I	Yok	N	Tek	N	99,671 %	28 saat
II	N	N+1(yedekli komponentli)	Tek	N+1	99,741 %	22 saat
III	N+1	N+1(yedekli komponentli)	Çift, biri aktif	N+1	99,982 %	1,5 saat
IV	2N	2N	Çift, biri aktif	2N	99,995 %	26 dakika

2.2. Bilgi Güvenliği

İletişim ortamlarının gün geçtikçe yaygınlaşması ile sanal ortamda bulunan bilgi bu gelişmeye paralel olarak artmıştır. Bu nedenle bilgilerin güvenliğinin sağlanma ihtiyacı üst seviyelere çıkmıştır. Bunun başlıca temel sebepleri arasında bilginin dünyanın hemen hemen her yerinde ağ ortamında bulunması sonucu bu ortamlarda oluşan güvenlik zafiyetlerinin olmasını söyleyebiliriz.

Kişi ve kurumların bilgi güvenliğini sağlamadaki eksikliklerinin yanında saldırganların saldırı gerçekleştirebilmeleri için gereksinim duydukları yazılımlara veya araçlara internet üzerinden fazla bir bilgi birikimine ihtiyaç duymadan rahatlıkla erişebilmeleri ve daha önemlisi kişisel ve kurumsal bilgi birimlerine

yapılan saldırılardaki önemli artışlar, hem kişisel hem de kurumsal bilgi güvenliği hususunda yeni güvenlik yaklaşımlarına daha fazla önem verilmesi zorunluluğunu ortaya çıkarmıştır [17].

Bilgi güvenliği, bilginin işlenebildiği, korunabildiği ve her türlü bilişim altyapı ortamında sağlanmak zorundadır. Bilginin muhafaza edilmeye çalışıldığı ilk andan itibaren güvenlik zinciri tabiriyle en zayıf halkasını her zaman insanlar oluşturmuşlardır [18]. Genel bir söylem olan "gücünüz en zayıf halkanız kadardır" ilkesi bilgi güvenliği için de geçerlidir [19].

2006 yılı itibaren ortaya çıkan ve günümüzde de hala etkin bir şekilde saldırganlar tarafından kullanılan oltalama (phishing) tekniği etkili bir sosyal mühendislik temelli saldırı yöntemi olarak söylenebilir. Geçmiş yıllarda bilgi teknolojilerine en büyük zarar veren virüs saldırıları son yıllarda yerini sazan avlama tekniklerine bıraktığını söyleyebiliriz. Bu yöntemde bilgi teknolojileri hususunda çok yetkin olmayan kurbanlar seçilerek sahte hesaplar veya sahte iletişim kanalları üzerinden bu kurbanlar dolandırılmaktadırlar veya taciz edilmektedirler.

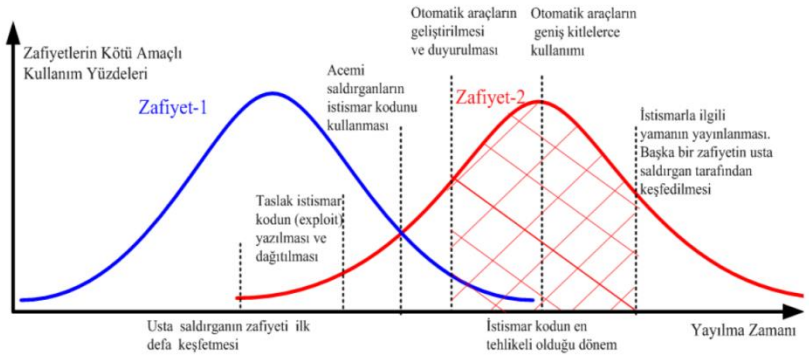
2.2.1. Kurumsal bilgi güvenliği

Kurum veya kuruluşlarda belirli bir güvenlik seviyesinin oluşturulmasına yardım eden güvenlik politikaları, tüm bilişim personelinin ve ortak çalışmalar yapan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür [20]. Kurumsal bilgi güvenliği politikası, kurum ve kuruluşlarda bilgi güvenliğinin sağlanması hususunda tüm bilişim altyapı güvenliğini ve diğer güvenlik faaliyetlerini kapsayan talimatlar olarak ve kurumsal bilgi kaynaklarına erişim izni olan tüm personelin uyması gereken kuralları içeren sertifikalı belgeler olarak söylenebilir [17].

2.2.1.1. Kurumsal bilgi güvenliği ve güvenlik testleri

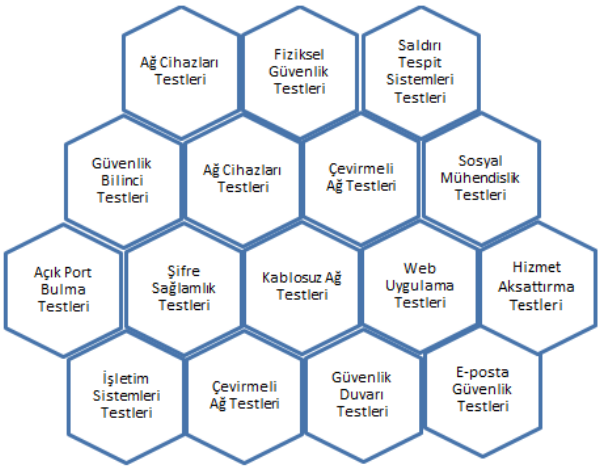
Kurumlara ait binlerce veya milyonlarca verinin güvenliğinin sağlanması hususunda kurum yöneticileri çok hassas ve tedbirli hareket etmektedirler. Bazen olası bir

saldırı sonucunda oluşabilecek hasarı karşılamak mümkün olamayabilir. Bu bağlamda kurumsal bilgi sistemlerinin güvenliğinin sağlanmasında güvenlik açıklarının önceden tespitinin önemi büyüktür. Saldırı gelmeden önce zafiyetlerin tespit edilerek güncellenmesini sağlayan güvenlik testleri kurumsal bilgi güvenliğinin sağlanması açısından büyük önem taşımaktadır. Güvenlik testlerinin madde madde sınıflandırılarak kurumların ya da kişilerin ihtiyaçları noktasında sosyal etik kurallara saygılı güvenlik personelleri tarafından yapılması güvenlik testlerinin başarılı olması açısından önem arz etmektedir [21]. Bu testlerin amacı kurumsal bilgi sistemlerine düzenlenebilecek saldırıları, saldırgan gözüyle kontrollü olarak saldırı gelmeden önce kontrollü saldırılar düzenleyerek gerekli tedbirlerin önceden alınmasında kurumlara yardımcı olmaktır.



Şekil 2.2. Zaafiyet Yaşam Süresi ([22]'den alınmıştır).

Şekil 2.2.'de görüldüğü üzere usta saldırganın bilişim altyapısında ilk zafiyeti keşfetmesi zamanına bilişim terimi olarak Zero-Day denilmektedir. Bu zamanın başlangıcı ile geçen süre zarfında bu güvenlik açığına uygun olarak geliştirilen otomatik araçların saldırganlar tarafından toplu bir şekilde kullanılması ile istismarın en etkili ve en tehlikeli olduğu zaman periyodu ortaya çıkmaktadır. Bu güvenlik açığının güncellenerek yama yapılmasına kadar geçen zaman zarfında saldırılar gerçekleşmekte ve büyük zararlar meydana gelmektedir.

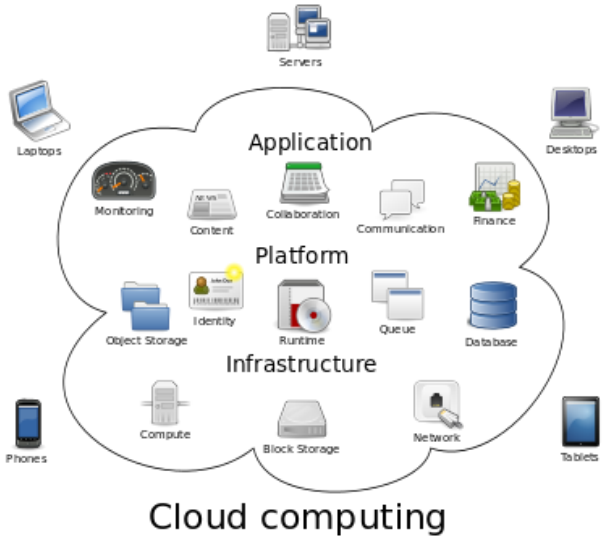


Şekil 2.3. Bilgi Güvenliği Testleri

Şekil 2.3.'de kurumlarda yapılan genel olarak Bilgi Güvenliği Testleri gösterilmiştir. Tüm bu yapılan güvenlik testlerine harcanan milyonlarca dolara rağmen bazen saldırılar yine engellenememekte ve yine milyonlarca zarar meydana gelmektedir. Sürekli gelişen teknolojiyle beraber gelişen bu saldırı araçları ve saldırı yöntemleri ile saldırganların ne derece engellenebilir olduğu sorusunu akıllara tekrar tekrar getirmektedir. 1 saniye bile hizmet kesintisi sonucunda astronomik paralar ödeyen servis sağlayıcı bu kurumlar, bazı durumlarda bile bu riski göze almak zorunda kalmaktadırlar. Bu sebeple Bölüm 3'de geliştirdiğimiz model, bu riski azaltmayı amaçlamaktadır.

2.3. Bulut Bilişim

Bulut bilişim (Cloud computing) veya kullanım manasıyla çevrim içi bilgi dağıtımı; bilişim cihazlarının birbirleri arasında özel veya özel olmayan bir bilgi paylaşımını sağlayan hizmetlere verilen genel bir isim diyebiliriz. Diğer bir tanımlama ile bulut bilişim bu bağlamda bir üründen çok hizmettir denilebilir. Altyapıda yer alan temel yazılım ve bilgilerin paylaşımının ve bilişim servislerinin bilgisayarlar ve diğer cihazların bağlı olduğu bilişim ağı (tipik olarak İnternet'ten) üzerinden kullanılmasıdır [23].



Şekil 2.4. Bulut Bilişim ([23]'den alınmıştır).

Dünya geneline bakıldığında 2014 yılında bulut bilişime 4,4 milyar dolar yatırım yapan Kanada listenin ilk sırasında yer almaktadır. 2018 yılına kadar bulut bilişime ayırdığı 11,5 milyar dolarlık bütçeyle Japonya ikinci sırada, 3,2 milyar dolarla İngiltere ve 1,1 milyar dolarla Brezilya izlemektedir [24]. ABD'nin yaklaşık 3 yıl önce açıkladığı demeçte ABD'de yer alan kurumların bulut bilişim harcaması 2014 yılında beklenen 2,2 milyar dolarlık harcamanın üzerine çıktığını ve bu ek harcamanın yaklaşık 800 milyon dolar gibi bir rakamın üzerine çıkıldığını belirtti [25]. Bu bağlamda değerlendirme yapıldığında ABD gibi birçok gelişmiş ülkelerin kamu kurum ve kuruluşlarında bulut bilişim sistemlerine geçişin daha hızlı olduğu söylenebilir ve bu doğrultuda Türkiye'nin de ufak da olsa atılımları görülmektedir. NIST(Amerikan Ulusal Teknoloji ve Standartlar Enstitüsü)'e göre Bulut Bilişim'i ulaşılması çok rahat olan, kullanılmaya hazır, kısa sürede bilgisayar kaynaklarının kullanıma hazır hale getirilip paylaşılabildiği ağ bağlantısı sağlama modeli olarak tanımlamıştır [26]. İstediğimiz herhangi bir zamanda bize sağlanan ağ bağlantısı sayesinde istediğimiz kaynaklara istediğimiz bir yerden bağımsız olarak ulaşabildiğimiz ve kaynak istemi arttıkça da ya da azaldığında kullanıcıya esneklik verebilen servisleri barındırırlar [26].

2.3.1. Bulut bilişim servis modelleri

2.3.1.1. Altyapı hizmetleri (Infrastructure as a service -IaaS)

Bulut teknolojilerinde en alt seviyede yer alan servis hizmetleri bütünü olarak tanımlanabilir. Altyapı hizmetlerinde altyapının ihtiyaç duyabileceği yük dengeleme servisleri depolama servisleri ve sanal makine migrasyonları gibi temel gereksinimleri ifade eder. Bu altyapı sayesinde kullanıcılara sanal donanımlar sunulmaktadır [27]. Bulut yazılım servisi bulut altyapısı üzerinde çalışabilir ve kullanıcı web tarayıcısı gibi araçlarla bu yazılım uygulamalarına ulaşabilir. Amazon EC2 bu modele örnek olarak gösterilebilir.

2.3.1.2. Platform hizmetleri (Platform as a service – PaaS)

Servis sağlayıcı, kullanıcıya kendi uygulamasını geliştirip, çalıştırabileceği bir ortam ve bu ortamın yanı sıra tamamlayıcı servisleri ve gerekli teknolojik altyapıyı da kapsayan bir platform sunar. Kullanan kişinin kendi kurduğu uygulama dışında, platform altyapısını oluşturan bileşenler üzerinde herhangi bir kontrolü ve yönetim imkânı yoktur [28]. Bulut Platformu Tüketici servis sağlayıcı tarafından sunulan yazılım dilleri ve araçlarını kullanarak bulut altyapısı üzerinde kendi yazılımlarını geliştirebilir ve sadece kendi geliştirdiği yazılımlara ve yazılımın barındırılması için gerekli çevre birimleri üzerinde kontrol ve yönetime sahiptir. IBM firmasının Bluemix bulut altyapısı, firmalara sağladıkları uzaktan erişim bulut platformları bu kategoriye örnektir.

2.3.1.3. Yazılım hizmetleri (Software as a service – SaaS)

Yazılım Hizmetleri servis modelinde kullanıcıların bulut uygulamalarının bulunduğu seviyeyi temsil eder. Kullanıcılar internet üzerinden kısıt olmaksızın istediği zaman bu uygulamalara web tarayıcıdan veya mobil cihazlardan erişerek kullanabilir. Genel olarak ifade etmek gerekirse bulut serviste yer alan yazılımların bulut altyapısını kullanarak çalıştığı ve bu uygulamalara kullanıcıların eriştiği katman olarak ifade

edilebilir. Basit bir e-posta hizmetinden, muhasebeye, finansa veya oyun uygulamalarının bulunduğu web-tabanlı kurumsal veya son kullanıcı ilgilendiren tüm yazılımların güncel haliyle birlikte hizmet olarak sunulduğu modeldir [29].

2.3.1.4. Servis olarak bulut (Cloud as a service- CaaS)

Kullanıcılara ait ürünler, servisler veya uygulamalar internet üzerinden gerçek zamanlı olarak servis edilir. Bulut servis altyapısı genel olarak diğer servis modellerinin tamamını kapsadığı söylenebilir. Herhangi bir mağaza için standart olarak önceden hazırlanmış veya kurulumu yapılmış olarak paylaşılan bir servistir.

2.3.2. Bulut bilişim hizmet modelleri

Bulut bilişim hizmet modellerinin kullanılma biçimleri yönünden de kategorilere ayrılabilir. Bunlar Genel (Public Cloud), Özel (Private Cloud), Topluluk (Community Cloud) ve Melez (Hybrid Cloud) olmak üzere 4 bölüme ayrılmaktadır.

2.3.2.1. Genel bulut (Public cloud)

Bulut bilişim hizmetleri içerisinde kullanımı en yaygın olan ve genel kullanıma açık manasına gelen genel bulut hizmetleri kullanıcıların internet üzerinden kullanımını sağlayan hizmetlerdir. Bu hizmetler ücretsiz erişimlidir veya kullanım başına ödeme modeliyle ücretlendirilirler ve kullanıcı birimler, web uygulamaları üzerinden hizmetlere erişmektedirler. Örneğin Amazon, Google, GoGrid v.b. RightScale'ın raporuna göre genel bulutta kullanılan 1000 ve üzeri sanal makine yüzdelerindeki artış oranı %13'den %27'ye yükselmiştir ve bu oranın daha da artacağı belirtilmektedir [30].

2.3.2.2. Özel bulut (Private cloud)

Özel bulut sadece tek bir kurum veya kuruluş için sağlanan bulut altyapısıdır, dâhili olarak veya üçüncü parti uygulama tarafından yönetilebilir ve yine içeriden veya harici olarak barındırılabilir [23]. Özel bulutlar genel olarak eleştirilerin odak noktası olabilmektedirler. Bu durumun sebebi ise kullanıcılar bu hizmeti aldıktan sonra devamlı olarak kurmak ve yönetmek zorundalar hatta daha az aktif katılımlı yönetim modellerinden faydalanamamaktalar [23]. Özel bulut felsefesinde ise bu hizmete bu kadar merak uyandırıcı yapan temel sebep sunduğu uzun süreli ekonomik modeldir. Yine RightScale'ın raporuna göre genel bulutta kullanılan 1000 ve üzeri sanal makine yüzdelerindeki artış oranı %22'den %31'e yükselmiştir [30].

2.3.2.3. Topluluk bulutu (Community cloud)

Bu bulut bilişim modelinde birden fazla ortak hareket eden kurum veya kuruluşların ortak bir bulut sistemi altyapısını paylaşmalarıdır. Burada ortak olan kurum veya kuruluşlar topluluk olarak nitelendirilmekte ve bu topluluk üyeleri bulut bilişimdeki uygulamalara ve bilgilere erişebilmektedir. Örnek olarak devlet kuruluşlarının ortak bir bulut altyapı kullanmasında birleşmesini sağlayan E-Devlet uygulamasını söyleyebiliriz.

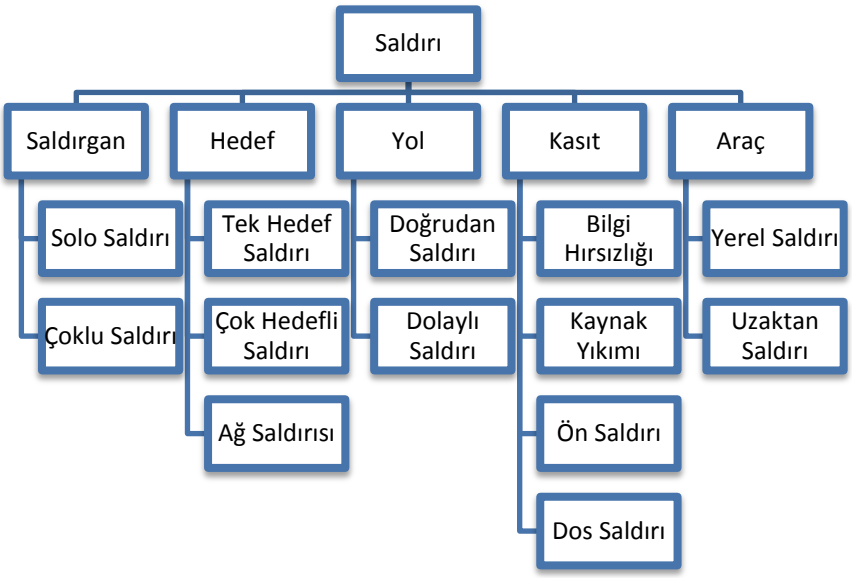
2.3.2.4. Melez bulut (Hybrid cloud)

Melez bulut iki veya daha fazla bulutun birleşimi olarak tanımlanabilir. Esas olarak bu birleşimde farklı bulut altyapısını barındıran veri merkezleri birbirlerine bağlanarak hizmet verir. Böylece bulut çoğullama ile farklı model imkânları sunarlar. Melez bulut mimarisi, kullanıcıların internet bağlantısına ihtiyaç duymadan lokasyon bağımsız anlık olarak kullanılabilme imkânı sağlar. Melez bulut mimarisi hem kurum içi bilişim altyapı kaynaklarına hem de bulut altyapısı gibi dış kaynaklara ihtiyaç duyar.

Tüm bu bulut modellerini incelediğimizde son yıllarda ciddi oranda sanal makine kullanımında artış olduğu söylenebilir. Bu sebeple sanallaşmanın bu şekilde yaygınlaşması ile siber saldırı ibrelerinin bu yöne kayabileceğini çok rahat tahmin edebiliriz.

2.3.3. Siber saldırılar

Genel olarak saldırılar çeşitli kısıtlar çerçevesinde sınıflandırılarak incelenebilir. Bunlar saldırgan sayısı, hedef türü, kullanılan yol veya kasıt ve araçlara göre Şekil 2.5.'de gösterildiği gibi sınıflandırılabilir [31].

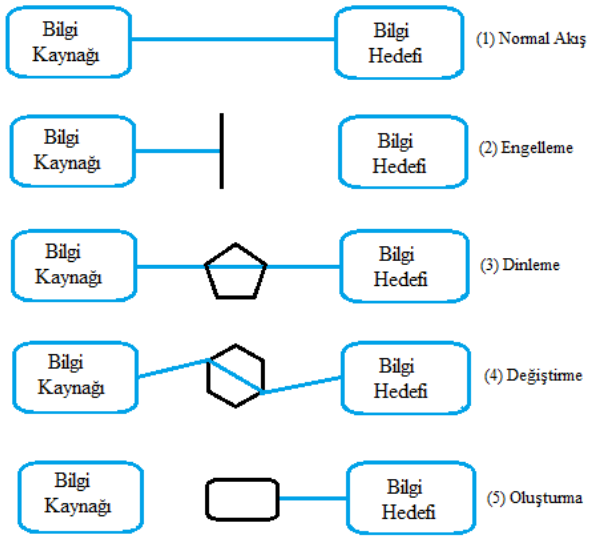


Şekil 2.5. Saldırıların Sınıflandırılması

1980 yılından itibaren son 35 senede yapılan saldırıların nitelikleri ve kapasiteleri incelendiğinde saldırganların bilgi seviyesi düşmesine rağmen saldırılar artmakta ve yine buna paralel olarak saldırı araçlarında da artış gözlemlenmiştir. Siber saldırılar zamanla ve gelişen teknoloji ile oldukça farklılıklar göstermektedir. Siber saldırılarda kullanılan araçlar, teknik açıdan gittikçe karmaşıklaşırken, bu saldırıyı yürütecek saldırganın ihtiyaç duyduğu bilginin seviyesi de gittikçe azalmaktadır. Bu durum saldırı ve saldırgan sayısını, saldırılar sonucunda oluşacak zararları artırırken, saldırıyı önlemek için yapılması gerekenleri de zorlaştırmaktadır. Özellikle hizmet aksatma saldırıları son yıllarda saldırganların üzerinde yoğunlaştıkları bir saldırı türü

olarak karşımıza çıkmaktadır. Buradaki ana saldırı amacı servisi uzun süre servis dışı bırakarak kullanıcılara uzun süre hizmetlerin ulaşamamasıdır.

Bilgi kaynağı ve bilgi hedefi arasındaki bilgi iletişim temelli olan bulut sistemler ve uygulamalarda iletişimin engellenmesi ve değiştirilmesi amaçlı oluşabilecek saldırı tipleri Şekil 2.6.'da gösterilmiştir. Bulut Sistem altyapısının en çok etkilendiği ve maruz kaldıkları saldırı tiplerinin en başında "Engelleme" olduğunu söyleyebiliriz. Yüksek bant genişliklerine rağmen yüksek kapasiteli saldırılar tüm trafiği engelleyerek bulut hizmetlerinin aksamasına neden olabilmektedir. Sadece bu aksamalar sebebiyle yüksek maddi zararlar meydana gelmektedir.

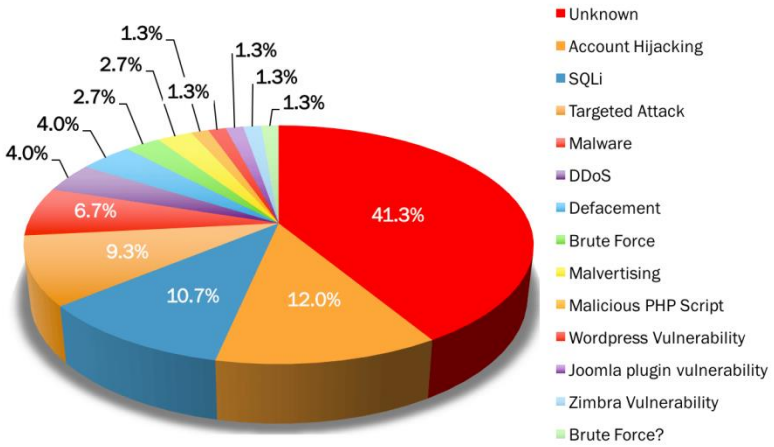


Şekil 2.6. İletişim Hedefli Saldırı Tipleri

Siber saldırıları düzenleyen kişilerin en motivasyon gücünün Siber Suç olduğunu söyleyebiliriz. Bunlardan en önemlisi dolandırıcılık ve yasa dışı hak edinme yöntemleri gibi başka insanların veya kurumların bilgileri ile para kazanma içgüdüsü olmaktadır. Saldırı nedenleri sıralamasında, Siber Suçları sırayla Siber Casusluk, Siber Savaşlar ve Hacktivism takip etmektedir.

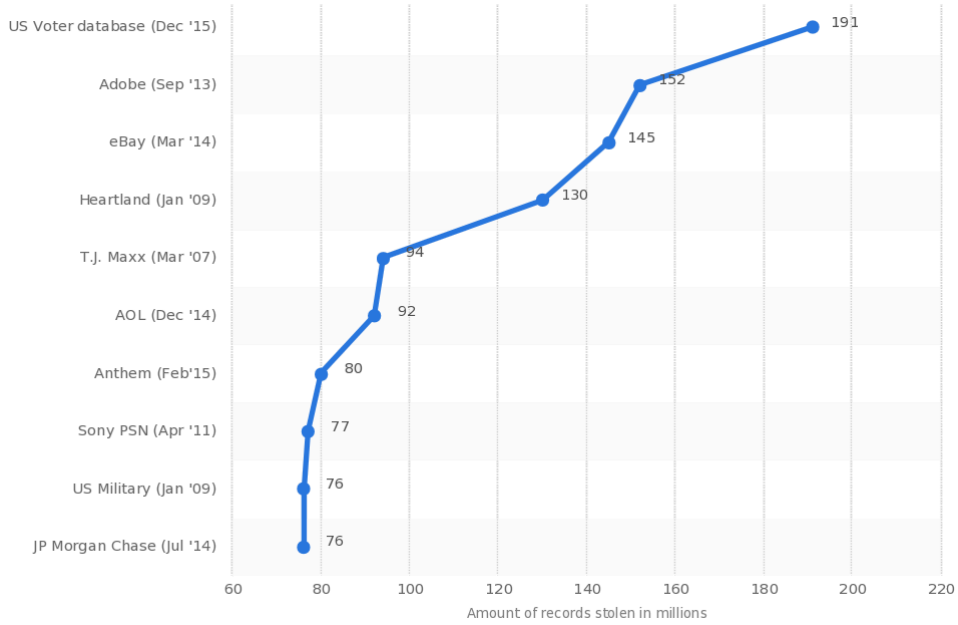
Hackmageddon isimli bir istatistik sitesinde, Şekil 2.7.'de de görüldüğü üzere Şubat 2016'da yapılan bir istatistik sonucunda siber saldırılarda kullanılan saldırı

tekniklerinin ilk sırasında %41,3 ile bilinmeyen teknikler yer almakta. Bunun ilk sırada olmasının sebebi saldırıya maruz kalan hizmet sağlayıcıların saldırının sebebini tespit edememelerinden kaynaklı olduğunu söyleyebiliriz. İkinci sırada %12,0 ile Hesap Korsanlığı ve üçüncü sırada ise %10,7 ile SQL injection yer almaktadır. Buradan anlaşılıyor ki hizmet sağlayıcıları veya kurumlar her ne kadar önlem alırlarsa alsınlar gelişen teknoloji ile birlikte güvenlik açıkları da artacak saldırılar kaçınılmaz olacaktır.



Şekil 2.7. Şubat 2016 Saldırı Kullanılan Saldırı Teknikleri İstatistiği ([32]'dan alınmıştır).

Şekil 2.8.'de Statista'nın yaptığı istatistikte ise geçmiş yıllardan günümüze kadar olan sürede bazı kurum ve kuruluşların maruz kaldıkları siber saldırı sonucunda çalınan kayıtların milyon cinsinden grafiğe dökülmüş halini göstermektedir. Bunlardan bazılarını ele alırsak Amerikan ordusundan Ocak 2009'da 76 milyon, Adobe şirketinden Eylül 2013'de 152 milyon ve eBay şirketinden Mart 2014'de ise 145 milyon kayıt çalındığı rapor edilmiştir. Sadece bu verilere bakarak olası bir saldırı ile bir anda milyonlarca kayıtların çalınabileceğini ve kötü niyetli olarak kullanılabileceğini söyleyebiliriz. Mart 2016'da da yine aynı şekilde ülkemizde yaklaşık 50 milyon kişinin kimlik bilgilerinin çalındığını ve bunların internet ortamında paylaşıldığı bilinmektedir [33].



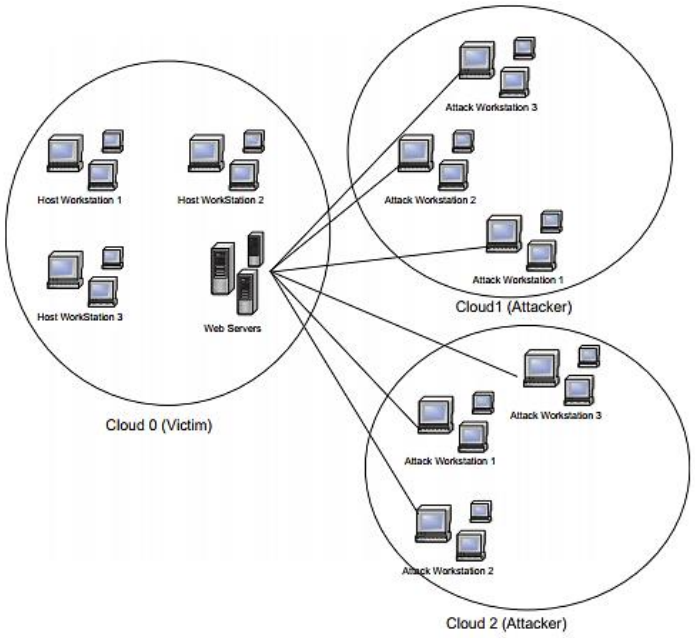
Şekil 2.8. Siber Saldırı Sonucunda Kurumlarda Meydana Gelen Veri Kayıpları [34].

2.3.3.1. Bulut bilişime yapılabilecek olası saldırılar

Özellikle son yıllarda bulut bilişimin yaygınlaşması ile bulut bilişim teknolojileri siber saldırıların odak noktası haline gelmiştir. Bu saldırılar için birçok yöntem ve teknik geliştirilmiş ve hala da geliştirilmektedir. Saldırganların en çok odaklandıkları nokta ise bulut servisleri olmaktadır.

Bulut bilişime yapılan saldırılar ile ilgili yapılan literatür araştırmasında birçok güncel çalışma mevcuttur. Bunlardan, Ajey Singh ve Dr. Maneesh Shrivastava yaptıkları çalışmada bulut bilişimden ortaya çıkabilecek güvenlik açıklarını ele almışlardır [35]. Bu saldırıları, "Denial of Service (DoS) Attacks", "Cloud Malware Injection Attacks", "Side Channel Attacks", "Authentication Attacks" ve "Man-In-The-Middle Cryptographic Attacks" 5 ana kategoriye ayırmışlardır. Diğer bir çalışmada da bulut kaynaklarının ve hizmetlerinin kullanılabilirliği, gizliliğini ve bütünlüğünü etkileyen farklı müdahaleleri "Insider Attacks", "Flooding Attacks", "User to Root Attacks", "Port Scanning", "Attacks on Virtual Machine (VM) or Hypervisor" ve "Backdoor Channel Attacks" şeklinde 6 bölüme ayrılmıştır [36]. Bu saldırıları tespit edecek yöntemleri ise Cloud Saldırı Tespit Sistemleri (IDS) ve

Saldırı Önleme Sistemleri (IPS) olmak üzere 2 bölüme ayrılmıştır. Bu çalışmada özetle, bulut sistemlerde saldırı tespit mekanizmalarının en verimli şekilde işlemesi için IDS ve IPS sistemlerinin hangi şartlar altında hangi bölgelere entegre edilmesi gerektiği anlatılmıştır. Bu bağlamda olası bir saldırıya karşı Bölüm 3'de önerdiğimiz modelin optimum olarak çalışabilmesi için erken uyarı sistemleri ile bütünleşik olması gerekmektedir. Erken uyarı sistemleri ile tasarlanan modelin entegrasyon seviyesi modelin başarımını ortaya koyacaktır.



Şekil 2.9. Bulutlar Arası Saldırılar ([37]'den alınmıştır).

Şekil 2.9.'da iki farklı bulut sistemden başka bir bulut sisteme yapılan saldırı modeli gösterilmiştir. Bu saldırı tipinde Xml tabanlı DoS saldırı yöntemi kullanılmıştır. Bu yöntemle kurban bulut sistem üzerinde çalışan servislerin band genişlikleri daraltılarak veya bu servislerin direk yanlış çalışması sağlanarak saldırı gerçekleştirilebilmektedir.

2.3.4. Sanallaştırma

Günümüz bilişim teknolojilerinden en popülerlerinden birisi olan sanallaştırma teknolojisi sanallaştırma özelliğine sahip işlemcilerin yaygınlaşması ve bu platformlar için güçlü ve performanslı bilgisayar donanımların üretilmesi sayesinde

sunucuların veya iş istasyonları gibi evimizde bulunan bilgisayarların sanallaştırma adına son kullanıcının da yer aldığı test ortamları oluşturulabilmektedir. Bazı şirketler veya bireysel kullanıcılar ise bütçeleri oranında donanım veya depolama birimleri satın alarak sanallaştırma altyapısını kendi ürün ortamlarında da kullanabilmektedirler. Bugün hemen hemen her yerde sanallaştırma teknolojisine geçmiş ve fiili olarak kullanan orta ve büyük ölçekli şirketler görebiliriz.

Birden fazla fiziksel bilgisayar yerine yüksek özelliklere sahip tek bir bilgisayar kullanarak aynı verim elde edilebilir ve sistemler kurulabilir. Bu sayede donanımsal olarak kablolama, soğutma ve sunucuların kapladığı büyük alanlardan tasarruf sağlanmaktadır [38]. Herhangi bir afet veya bir arıza olması durumlarında sistem arıza süresini saniyelere kadar indirmektedir.

Tablo 2.2. VMware ESX İle Sanallaştırılan Veri Merkezinin Tasarruf Oranları [38].

Fiziksel Altyapı	Sanal Altyapı	Kazanç Oranı
37,248 Server	776 ESX Host	48:1
2483 Rack	28 Rack	88:1
25MW Power	0,5MW Power	48:1
6208 Core	74,496 Virtual CPU	1:12

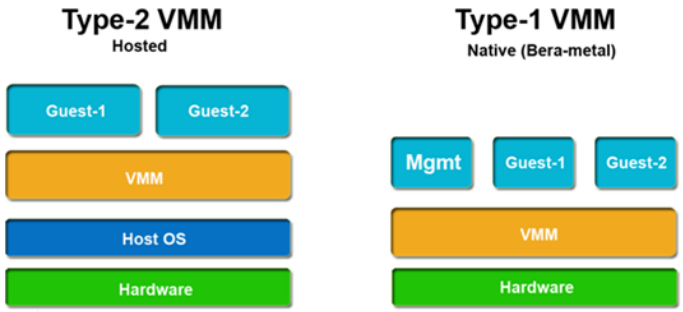
Tablo 2.2'de gördüğünüz üzere 37,248 Fiziksel Sunucu yerine 776 Adet VMware ESX ile sanallaştırılmış sunucu kullanılarak 48 kat enerji tasarrufu sağlanmıştır ve 2483 Rack yerine de 28 Rack kullanılarak ise 88 kat yer tasarrufu sağlanmıştır [38].

2.3.5. Hypervisor nedir?

Fiziksel bir sunucu üzerinde birden fazla sanal makinenin çalışmasına olanak sağlayan ve bu sanal makinelerin çalıştırılmasına altyapı sağlayan yazılıma hypervisor denir. Diğer bir tanımla, hypervisor birden fazla işletim sisteminin aynı donanım üzerinde aktif olarak çalışmasını sağlayan ve boyutu küçük kod parçacıkları olarak denilebilir [39].

Fiziksel sunucu üzerinde sanal makineler oluşturmak için veya diğer bir adla sanallaştırma yapabilmek için hypervisor altyapısının kurulu olması gerekmektedir. hypervisor kurulumu ile fiziksel makine üzerine kurulan işletim sistemi artık bir ana bilgisayar olarak çalışmaktadır [39]. Fiziksel sunucu ilk açıldığında ilk önce hypervisor açılacak ve ardından ana bilgisayarda olan ana işletim sistemi açılacaktır [39].

Hypervisorlar kendi aralarında Şekil 2.10.'da görüldüğü üzere 2 ye ayrılmaktadır. Bunlar Type-1 ve Type-2'dir.



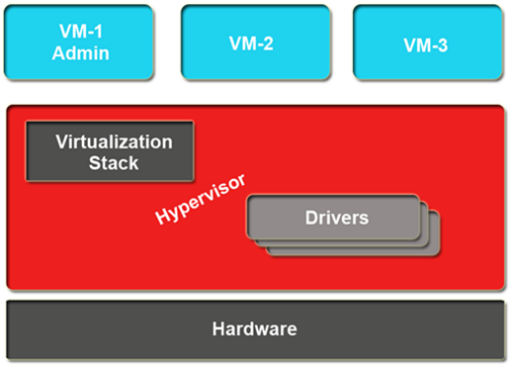
Şekil 2.10. Type-1 ve Type-2 Hypervisor [39]

2.3.5.1. Type-1 hypervisor

Yazılım direk olarak fiziksel sunucu üzerine kurulur ve oluşturulacak sanal makineler ise hypervisor yazılımının üzerinde kurulur. Bu tip hypervisor'ların en olumlu yönü direk olarak fiziksel sunucu üzerinde çalışmaları sebebiyle fiziksel sunucunun kaynaklarının hemen hemen tamamını kullanması ile performans açısından sağladıkları yüksek verimdir. Kurumsal firmalarda ve ürün testi ortamlarında kapsamlı sonuçlar alınması açısından önemli olduğu için kullanılan hypervisor tipidir. Microsoft Hyper-V, VMware vSphere ESX/ESXi ve Citrix Xen Server bunlara örnek olarak verilebilir. Type-1 hypervisor'lar kernel ve yazılım yapılarına göre ikiye ayrılmaktadırlar.

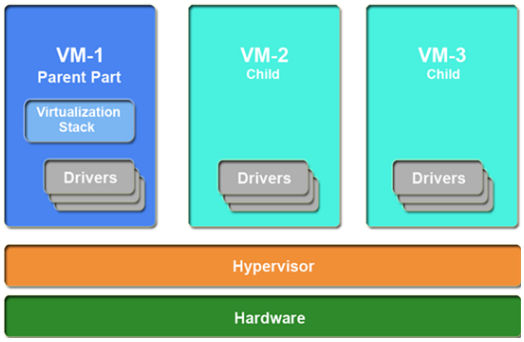
- Monolithic hypervisor: Yapısında bir fiziksel makinede kurulu ana işletim sistemine ihtiyaç duyulmaz. Hypervisor uygulaması direk olarak fiziksel donanım üzerine kurulur ve ardından kurulan sanal makineler de hypervisor

ile direk olarak iletişim halindedir. Bu hypervisor tipleri karmaşık bir kernel yapısına sahiptirler [39]. Üreticilerin kendi driver'ları monolithic hypervisor içerisinde yer almaktadır [39]. Sanallaştırma bölümleri hypervisor içerisinde yer aldığı için bu hypervisor yapıları çok geniş yer kaplamaktadır [39]. Donanım üzerinde kurulu tüm sanal makineler hypervisor ile direk olarak haberleştiğinden, hypervisor üzerinde kurulduğu fiziksel donanım için tüm sürücüleri de içermek zorundandır. Bu sayede desteklenen donanım çeşidini en aza indirgediğinden bu tip hypervisor'ın kurulacağı fiziksel donanımın teknik özellikleri iyi incelenmelidir. Monolithic hypervisor tipine örnek olarak VMware firmasının ESX ve ESXi ürünleri gösterilebilir. Şekil 2.11. bize monolithic hypervisor yapsını daha iyi kavrayabilmek için yardımcı olacaktır.



Şekil 2.11. Monolithic Hypervisor [39]

- Microkernelized hypervisor **:** Microkernelized hypervisor tipleri adından da anlaşılacağı üzere çok küçük bir yapıya ve boyuta sahiptirler. Asgari ve azami olarak hesaplandığından ortalama 1,5 Megabayt'lık bir boyuta sahip olduğu söylenebilir. Microkernelized hypervisor'ler içerisinde üçüncü parti bir yazılım bulundurmazlar. Şekil 2.12.'de de görüldüğü üzere sürücüler, misafir işletim sistemleri üzerinde yer aldığından dolayı bu tip hypervisorlar'ın daha güvenli olduğu söylenebilir. Örnek olarak Microsoft firmasının üretmiş olduğu Hyper-V örnek olarak verebilir.



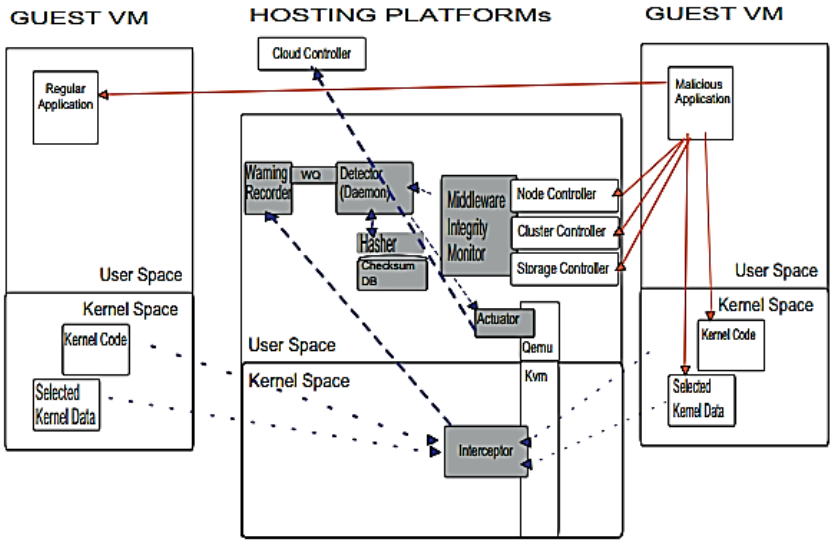
Şekil 2.12. Microkernelized Hypervisor [39]

2.3.5.2. Type-2 hypervisor

Bu hypervisor tipinde fiziksel sunucudaki kurulu ana işletim sistemi üstüne kurulur ve işletim sisteminin üzerinde bir katman olarak çalışır. Bu hypervisor'ın en büyük dezavantajı ise katman seviyesinde kaldığı için performans kayıplarının yaşanması ve fiziksel sunucunun yüksek kapasitelerinden yararlanamamasıdır. Bu sebeple genel olarak temel seviyede test ortamlarında kullanılmaktadır. Bu hypervisor tiplerine ise Microsoft Virtual Server, Microsoft Virtual PC, VMware Server ve VMware Workstation ürünleri örnek olarak verilebilir.

2.3.6. Ev sahibi-misafir makine bağlantılı olası saldırılar

Sanal makineler çalışma zamanlarında saniyede yaklaşık 600 kez sanal makine çıkışları yapabilmektedirler [40]. Bu sanal makine çıkışlarını hypecall olarak da tanımlayabiliriz. Bu çıkışların 56 farklı teknik sebebi mevcuttur. Bunların hemen hemen hepsi sanal makinelerin çekirdek (kernel) ile hypervisor üzerinden iletişime geçmeleri veya donanımsal olarak sürücü bağlantılarının sağlanması amaçlı olabilir. Bu gibi birçok nedenden dolayı fiziksel makineye açılan kapı olan bu kanallar sebebiyle sanal makineler üzerinden saldırılar mümkün olabilmektedir.



Şekil 2.13. Sanal Makine Üzerinden Fiziksel Makineye Erişim [41]

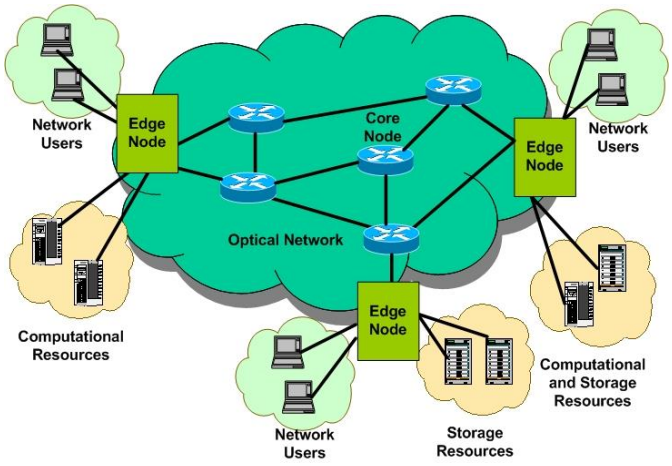
Şekil 2.13.'de görüldüğü üzere misafir sanal makine (Guest Vm) üzerinden zararlı yazılımlar ile direk olarak barındırıcı makineye(Hosting Platform) müdahale söz konusu olabilmektedir. Bu zararlı etki direk kernel yani çekirdek koda olabilir ya da barındırıcı makine üzerindeki kontrol uygulamalarına da mümkün olabilmektedir.

BÖLÜM 3. PROBLEM TANIMI VE FORMÜLASYONU

Bu bölümde önce problemin tanımı yapılmış, sonra da çözümü için geliştirilen ILP formülasyonu verilmiştir. En sonunda da örnek bir senaryo üzerinden formülasyonun nasıl çalıştığı gösterilmiştir.

3.1. Problem Tanımı

Optik ağ bir telekomünikasyon ağının çeşitli düğümler arasında bilgi iletimi için ışığa kodlanmış sinyalleri kullanan bir iletişim aracıdır [42]. Şekil 3.1.'de iletişim altyapı mantığı anlatılan Fiber Optik Ağlar yerel alan ağlarında ya da ulusal, uluslararası ve okyanus ötesi mesafelere kadar bir geniş alan ağı (WAN) üzerinde çalışabilir. Optik erişim ağları üç değişik şekilde düzenlenebilmektedir [43].



Şekil 3.1. Fiber Optik Ağ Omurgası [44]

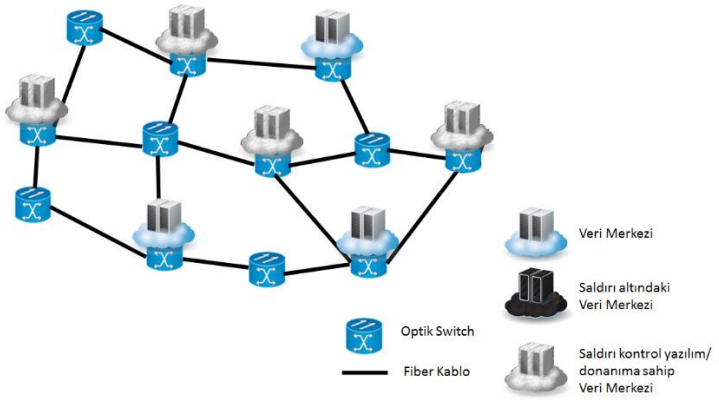
1. Noktadan Noktaya Bağlantılı Ağlar
2. Aktif Yıldız Bağlantılı Ağlar
3. Pasif Yıldız Bağlantılı Ağlar (PON)
    a. APON – BPON
    b. GPON

c. EPON – GEPON – 10G EPON
d. NGPON

Son yıllarda öne çıkan GPON teknolojisi özellikle ülkemizde de Turkcell Superonline Türk Telekom TTNET gibi şirketlerinin üzerinde durduğu ve pasif ekipmanla çalışan bir teknoloji olduğunu söyleyebiliriz. En önemli avantajı ise iletişimin yüksek hızda ve yüksek kapasitede olmasıdır.

CISCO'nun yaptığı araştırmaya göre 2013 yılında internette akan verinin 667 Exabyte olduğu saptanmıştır. Böylesine yüksek verinin internet ortamında dolaşmasına fiber optik ağların yüksek hızlı kapasiteli iletişim altyapısı sağlamaktadır. Saniyede 3.10^8 metre yol kat edebilen ışık hızı sayesinde yüksek veri kümeleri bir yerden başka bir yere hızlı ve güvenli bir şekilde iletilebilmektedir. Bu yüksek iletişim gücünün sağladığı faydaların yanı sıra zararlarının olduğunu da söylemek yanlış olmaz. Siber saldırılarda saldırganların son yıllarda tercih ettiği saldırı kaynaklarının hemen hemen hepsini artık fiber optik altyapısına sahip bulut sistemler oluşturmaktadır. Bu da saldırganlara önemli bir saldırı altyapısı sağlamaktadır.

Veri merkezleri optik ağ altyapısını kullanarak bir veri merkezi ağı oluştururlar. Bu veri merkezleri arasında veri alış verişi optik ağ üzerinde optik devreler (ışık yolları) kurularak mümkündür.



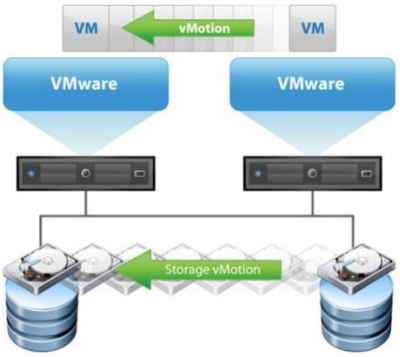
Şekil 3.2.Veri Merkezi Ağı Topolojisi

Şekil 3.2.'de de görüldüğü üzere örnek bir veri merkezi ağı topolojisi oluşturulmuştur ve bu topolojide farklı düğümler farklı lokasyonlarda da olabilir. Bu bağlamda olası saldırılarda saldırıdan kaçınma amaçlı olarak kurtarılması gereken bilgilerin farklı veri merkezlerine de aktarılması gerekebilir. Bu tahliye ve kaçınma yöntemi veri merkezlerinin hizmet altyapısını oluşturan sanal makinelerin migrasyon edilmesi ile kolaylıkla gerçekleştirilebilir. Bu tahliye yöntemi sayesinde saldırı altındaki veri merkezleri kısa sürede karantinaya alınması sağlanarak saldırının etki edeceği zarar önemli şekilde engellenebilir.

Sanal makine migrasyonu (VM migration), sanal makineler ister kapalı olsun ister açık olsun önemsenmeyecek ufak çaplı kesintiler dahilinde başka bir uzak makineye tüm bilgileri taşıma işlemine verilen addır. VMware, Xen vb. birçok sanal makine oluşturma olanağı sağlayan hypervisor tabanlı ürünler migrasyon işlemine olanak sağlamaktadır. Bu işlem önceden yedek alınmışsa sadece güncellemeler ile milisaniyeler içerisinde gerçekleşebilmekte ve böylece bu işlem sırasında kullanıcı bile bu durumu fark edememektedir. Farklı ürünlerin farklı migrasyon yöntemleri mevcuttur. VMware firmasına ait migrasyon yöntemlerini ele aldığımızda 5 farklı migrasyon şeklini aşağıdaki gibi sıralayabiliriz [45];

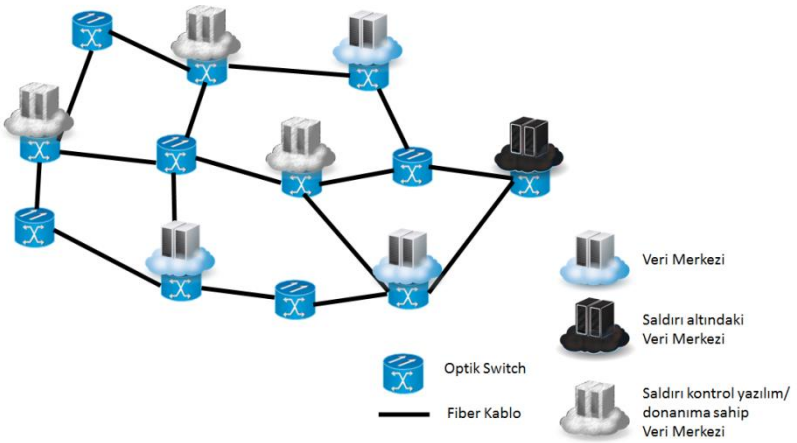
1. Cold Migration: Sanal makinenin kapalı iken sanal makine ve/veya sanal disklerin farklı veri merkezi üzerine taşınmasıdır. Depolama birimi paylaşımı gerekliliği yoktur. Farklı işlemci aileleri arasında olabilir.
2. Suspended Migration: Sanal makine askıda iken sanal makine ve/veya sanal disklerin farklı veri merkezi üzerine taşınmasıdır**.** Depolama birimi paylaşımı gerekliliği yoktur. Sadece aynı işlemci aileleri arasında olabilir.
3. Vmotion Migration: Şekil 3.3.'de migrasyon mantığı gösterilen Vmotion migration, sanal makinenin açık iken sanal makine ve/veya sanal disklerin farklı veri merkezi üzerine taşınmasıdır**.** Sanal makinelerin birden fazla host arasında paylaştırılarak yük dengelemesi yapılmasında veya fiziksel sunucuların bakımı durumunda kullanılabilir. Depolama birimi paylaşımı gerekliliği yoktur. Sadece aynı işlemci aileleri arasında olabilir [46].

4. Storage Vmotion: Sanal disklerin sanal makine ve/veya sanal disklerin farklı veri merkezi üzerine taşınmasıdır**.** Depolama birimi paylaşımı gerekliliği yoktur.
5. Enhanced Vmotion: Gelişmiş migrasyon tipi olup sanal makine açık iken sanal makine ve/veya sanal disklerin farklı veri merkezi üzerine taşınmasıdır**.** Depolama birimi paylaşımı gerekliliği yoktur. Sadece aynı işlemci aileleri arasında olabilir.



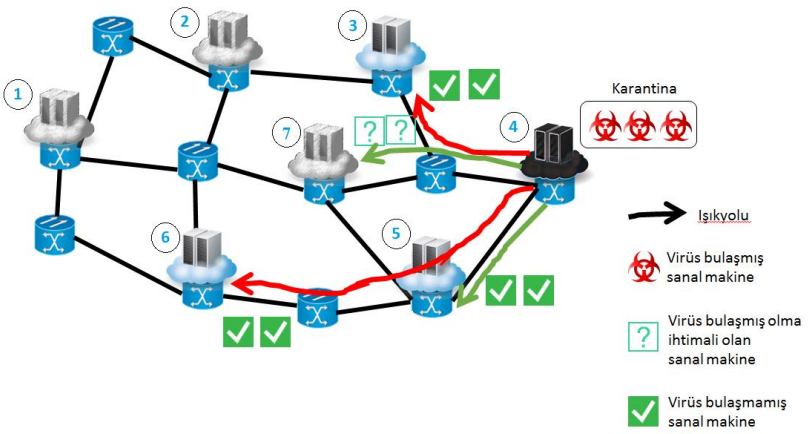
Şekil 3.3. vMotion İle Sanal Makine Migrasyonu [46]

Sanal makineler, vmotion, clone, storage vmotion yöntemleri ile migrasyon edilmesi gerekiyorsa bunları eş zamanlı olarak yapabilirler. Belirli firmaların belirli migrasyon yöntemleri mevcut olsa da gün geçtikçe daha hızlı ve daha stabil migrasyon yöntemleri geliştirilmektedir. Tahliye işlemlerinin en hızlı ve hatasız olması adına Enhanced migration yöntemi kullanılabilir.



Şekil 3.4. Saldırı Altındaki Veri Merkezi Ağı Topolojisi

Bu modelde Şekil 3.4.'de de görüldüğü üzere 7 farklı veri merkezin birbirleriyle optik ağ üzerinden bağlantıları sağlanmıştır. Veri merkezi ağında yer alan 4 numaralı veri merkezine bir siber saldırı olduğu görülmektedir. Yapılan bu saldırı ile 4 numaralı veri merkezindeki sanal makinelerden virüs bulaşma durumu olanlar hemen karantinaya alınırlar ya da kapatılabilirler.



Şekil 3.5. Sanal Makinelerin Tahliyesi

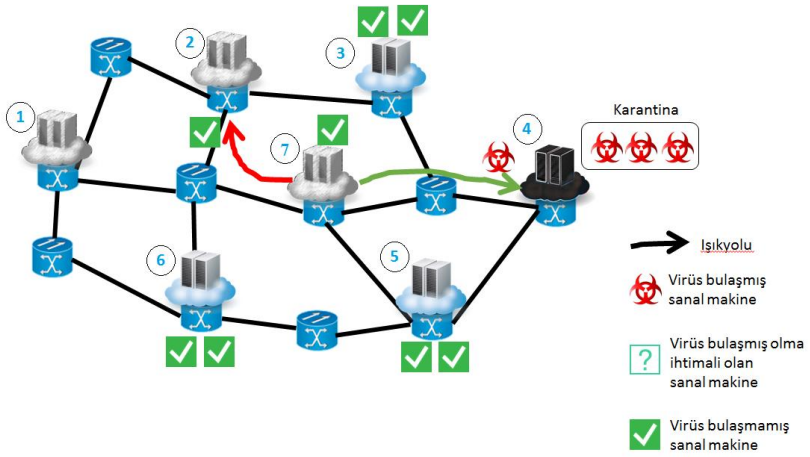
Genel olarak saldırıya uğrayan veri merkezindeki sanal makineler virüs bulaşıp bulaşmadığı noktasında hızlı bir kontrolden geçirilir ve üç gruba ayrılırlar;

1. Virüs Bulaşmış Olanlar
2. Şüpheli Durumda Olanlar
3. Güvenli Olanlar

Virüs bulaşmış olanlar karantinaya alınır. Şüpheli durumda olanlar kontrol için ilgili yazılım/donanım bulunan veri merkezlerine alınır. Virüs bulaşmamış olanlar ise diğer veri merkezlerine taşınır.

Şekil 3.5.'de de görüldüğü üzere 4 numaralı veri merkezine yapılan saldırıdan dolayı virüs bulaşmış sanal makineler karantinaya alınmıştır. Virüs bulaşmamış olan güvenli sanal makineler ise 3, 4, 5 ve 6 numaralı veri merkezlerine taşınmıştır.

Şüpheli durumda olan sanal makineler ise kontrol için ilgili yazılım/donanım bulunan 7 numaralı veri merkezine aktarılmıştır.



Şekil 3.6. Tahliye Edilen Sanal Makinelerin Kontrolü

Kontrolü yapılan sanal makineler eğer virüslü oldukları tespit edilmişse karantinaya alınır ve temizleme işlemi yapılır. Değilse aynı veri merkezinde tutulabileceği gibi başka veri merkezlerine de gönderilebilir.

Şekil 3.6.'da yapılan kontrol sonucunda virüs bulaşmış olan sanal makine 4 numaralı denetim merkezine aktarılıp hemen incelemeye alınmıştır. Virüs bulaşmamış olan sanal makine 2 numaralı güvenli veri merkezine transfer edilmiştir. Bu senaryoya göre buradaki ana hedef, olası bir siber saldırı esnasında mümkün olan maksimum sayıda sanal makinenin güvenli olarak migrasyonunun (tahliyesinin) gerçekleştirilmesidir.

3.2. Sistemin Genel Özellikleri ve Amacı

Sistemin temel amacı bulut bilişim altyapısına yapılacak olası bir siber saldırının tespiti ve elimine edilmesinden ziyade yayılımının önlenmesini sağlayacak bir çözümün geliştirilmesidir. Bir saldırı anında, bulut bilişim servislerinin bu saldırıdan minimum kayıpla kurtulması için hizmet kesintisi maliyetini de göz önünde tutarak müşterilerin, şirketlerin veya kurumların bu durumdan etkilenmesi minimize edilecektir. Böylelikle müşterilere, şirketlere veya kurumlara ait bilgilerde bozulma,

çalınma olayının bu yöntemle bertaraf edilmesi ve üretilen çözümün sanayi ve bilim camiasında siber güvenlik üzerine çalışan geniş bir kesime hitap etmesi planlanmaktadır.

Yapılan bu çalışmada belirlenen amaca ulaşılması için 2 temel hedef konulmuştur.

1. Tahliye probleminin zaman kısıtlamaları, veri merkezleri kaynakları ve ağ kaynakları göz önüne alınarak matematiksel olarak modellenmesi
2. Problem bir optimizasyon problemi olduğundan Lineer Programlama yöntemi ile değişik senaryolar ve farklı ağ topolojileri için GUROBI yazılımı üzerinden optimum sonuçların bulunması.

Ayrıca bu çalışmanın diğer bir amacı ise bulut bilişim sağlayıcılarının tehdit süreçlerinde tahliye edilecek hedef makineleri satın almak yerine kiralama veya farklı antlaşmalar üzerinden farklı sağlayıcılar ile iş ortaklığına gidebilmelerine imkân sağlayacak bir acil durum platformunun oluşmasına katkı sağlayacak olmasıdır.

3.3. Sistemin Matematiksel Olarak Modellenmesi

Belirlenen hedefler dâhilinde problemin öncelikli matematiksel olarak modellenmesi gerekmektedir. Bunun için de bir risk faktörü tanımlanması gerekmektedir. Burada risk, zararlı yazılımın yayıldığında ortaya çıkacak zarar olarak düşünülebilir. Bu zararı minimize etmek için de saldırı anında veri merkezindeki maksimum sayıda sanal makinenin güvenli şekilde tahliyesinin sağlanması gerekmektedir. Dolayısı ile problemin çözümünde amacımız güvenli sanal makine migrasyonunu maksimize ve maliyeti ise minimize etmek olacaktır.

Burada problemin değişkenlerini aşağıdaki gibi tanımlayabiliriz. Değişkenler;

V : Optik ağ düğümleri

D : Veri merkezleri $(D \subset V)$

K : Denetim merkezleri $(K \subset D)$

P : Düğümler arası yollar

R : Veri merkezleri arası rotalar

M_d : Düğümde yer alan sanal makineler

X_d : Eğer d düğümü saldırı altında ise 1;değilse 0

Q_d : Düğümdeki mümkün boş sanal makine kapasitesi

$W_{i,j}$: Fiberin bağlantı (dalga boyu) kapasitesi

$Y_{s,d}^{m}$: Eğer, W_m sanal makinesi s'den d' ye migrasyon oldu ise 1;değilse 0

$L_{s,d}^{r,m}$: Eğer sanal makine s veri merkezinden d veri merkezine r rotasını kullanarak migrasyon olmuş ise 1;değilse 0 $L_{s,d}^{r,m} = p, \forall p \in P$

Z_m : Eğer W_m sanal makinesi başarılı olarak güvenli yere taşınmış ise 1;değilse 0

B_m : Eğer W_m sanal makinesi virüs enfekte olmuş ise 1;değilse 0

T_m : Eğer W_m sanal makinesi şüpheli durumda ise 1;değilse 0

S_m : Eğer W_m sanal makinesi denetim altına alınmışsa 1;değilse 0

Pc_p : p yolu fiber maliyeti.

$Lc_{s,d}^{r,m}$: s düğümündeki veri merkezinden d düğümündeki veri merkezine r rotası kullanılarak yapılan sanal makine transferi için kullanılacak toplam maliyet

Problemin amacı sanal makinelerin taşınmasını maksimize etme ve maliyeti minimize etmek olduğu için pareto optimumundan kaçınma amaçlı maliyet fonksiyonuna çok küçük bir bir katsayı girilmiştir. Problemin amaç fonksiyonunu şu şekilde tanımlayabiliriz;

Amaç Fonksiyonu;

$$\max \left(\sum_{d \in D} \sum_{m \in M_d} X_d \left(Z_m + S_m \right) - \beta \sum_{s \in D} \sum_{d \in D} \sum_{m \in M_d} X_d \, Lc_{s,d}^{r,m} \right)$$

Burada β çok küçük bir sayıyı (örneğin 10^{-5}) ifade etmektedir.

Kısıtlar;

1. $$Z_m + S_m = Y_{s,d}^{m} \, X_s \left(1 - X_d \right), \forall s \in D, \forall d \in D, \forall m \in M_i$$

   Saldırı yapılan veri merkezindeki virüs bulaşmayan sanal makineler güvenli yere taşınmalı.

2.

- $Z_m \leq (1 - B_m) X_d , \forall d \in D , \forall m \in M_d$

  Sanal makine virüs enfekte olmuş ise güvenli taşıma olamaz.

- $Z_m \leq (1 - T_m) X_d , \forall d \in D , \forall m \in M_d$

  Sanal makine virüs şüpheli ise güvenli taşıma olamaz.

3.

- $S_m \leq (1 - B_m) X_d , \forall d \in D , \forall m \in M_d$

  Eğer saldırı altındaki herhangi bir sanal makineye virüs bulaşmamış ise denetime alınmasına gerek yok.

- $S_m \leq T_m X_d , \forall d \in D , \forall m \in M_d$

  Eğer saldırı altındaki herhangi bir sanal makine şüpheli değilse denetime alınmasına gerek yok.

4.

$$\sum_{s \in D} \sum_{m \in M_i} Y_{s,d}^m \leq Q_d \ \forall s \in D, \forall d \in D, \forall m \in M_d$$

Hedef düğümdeki mümkün boş sanal makine kapasitesi transfer edilecek sanal makinenin kapasitesinden büyük olmalı ve hedef düğümde mümkün boş sanal makine olmalı.

5.

$$\sum_{r \in E} L_{s,d}^{r,m} X_s = Y_{s,d}^m \ \forall r \epsilon R, \forall s \epsilon D, \forall d \epsilon D, \forall m \in M_d$$

Her sanal makine sadece bir rota üzerinden tahliye edilmeli.

6.

$$\sum_{r \in R} \sum_{p \in r} Pc_p X_s L_{s,d}^{r,m} = \sum_{r \in R} Lc_{s,d}^{r,m} \ \forall p \epsilon P, \forall r \epsilon R, \forall s \epsilon D, \forall d \epsilon D, \forall m \in M_d$$

En düşük maliyetli rotanın seçilmesi için rota üzerinde gidilecek yolların maliyetlerinin toplamı amaç fonksiyonunda minimize edilmeli.

7.

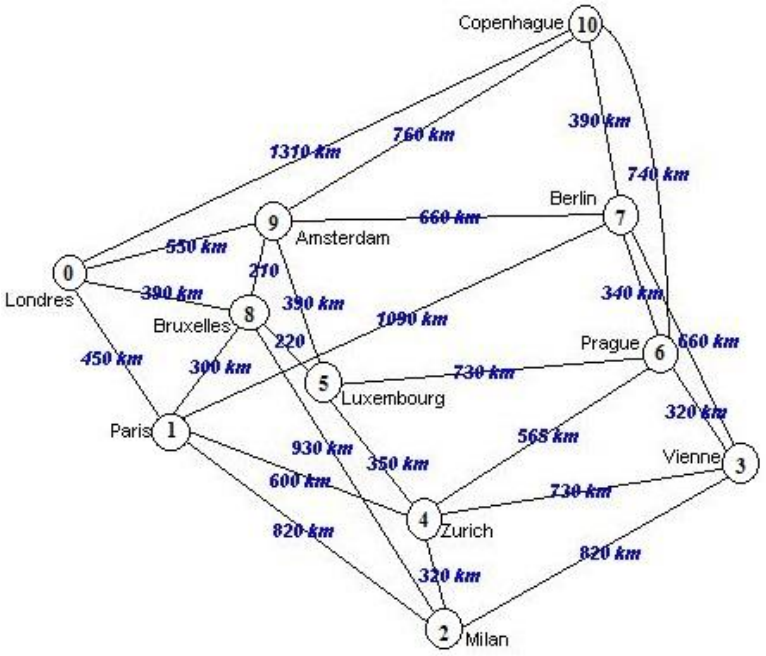
$$\sum_{s\in D}\sum_{d\in D}\sum_{m\in M_d} R_{s,d}^{k,lm} \leq W_{k,l}$$

Bağlantı üzerinde toplam bant genişliği kapasitesini aşmaması lazım.

3.4. Formülasyonun Çalışması ile İlgili Örnek Senaryo

Herhangi bir parametreyi minimize yada maksimize eden problemler optimizasyon problemleri olarak tanımlanabildiğinden bu tahliye problemi de Lineer Programlama tabanlı olan GUROBI v6.5 Api desteği ile JAVA'da kodlanarak çözümü yapılmıştır. Bu optimizasyon probleminin çözümünde Şekil 3.7.'de de görüldüğü üzere Avrupa şehirleri baz alınarak oluşturulan COST239 fiber optik ağı kullanılmıştır.

Oluşturulan matematiksel modelin GUROBI üzerinden çözdürülmesi için mevcut GUROBI optimizasyon paketleri ile kodlanması gerekmektedir. Bu çalışmada kodlama Java platformunda gerçekleştirilmiştir. Tüm problem değişkenleri GUROBI Api desteği ile Java'da tanımlanarak amaç fonksiyonuna uyarlanmıştır.

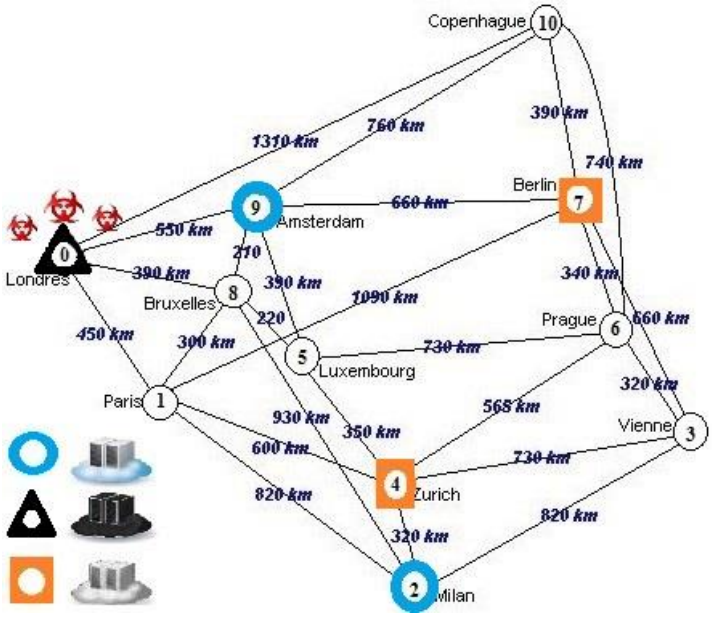


Şekil 3.7. 11 Düğümlü COST-239 Veri Merkezi Ağı Topolojisi

Problem 11 düğümlü bir veri merkezi ağı topolojisini içerdiği için bir düğümden başka bir düğüme giden birden fazla rota mevcut olacaktır. Bu mevcut rotaların tespiti için tüm mevcut rotaları tespit edecek bir algoritma olan Yen'in k en kısa yol algoritması kullanılmıştır. Bu algoritma ile rotalar sadece bir defaya mahsus olarak çalıştırılması yeterli olacaktır. Buradaki ana amaç programın optimizasyon çalışma zamanın kısaltılarak daha kısa sürede sonuç vermesini sağlamak olacaktır.

3.4.1. Örnek Senaryo

Kodlanan program, Şekil 3.8.'de görülen bir optimizasyon testine tabi tutulmuştur ve rasgele olarak sırasıyla Londra, Milan, Zurich, Berlin, Amsterdam olmak üzere 5 veri merkezi atanmıştır. Bu senaryoya göre Londra'ya yapılan bir siber saldırı olduğunu ve bu saldırı ile veri merkezine olası bir sızma veya zararlı yazılım bulaşma olduğu varsayılmıştır. Diğer veri merkezleri ise Amsterdam, Milan, Berlin ve Zurich olmuştur. Berlin ve Zurich veri merkezleri saldırı denetim merkezi olarak seçilmiştir. Saldırı durumunda Londra'daki veri merkezi saldırı tespit sistemleri verilen erken uyarı ile tahliye model uygulamamızı tetiklediği varsayılmıştır.



Şekil 3.8. 5 Veri Merkezli Saldırı Senaryosu

Londra veri merkezinde toplam sanal makine kapasitesi 10 olarak ve bu veri merkezinin doluluk oranı ise %50(Aktif 5 sanal makine) oranında belirlenmiştir. Şöyle ki;

- Sanal Makineler;
  $M_{Londra} = \{M_0, M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8, M_9\}$
- Aktif Sanal Makineler;
  $\{M_0, M_1, M_2, M_3, M_4\}$
- Aktif Olmayan Sanal Makineler;
  $\{M_5, M_6, M_7, M_8, M_9\}$
- Zararlı Yazılım Bulaşmış Sanal Makineler;
  $\{M_0\}$
- Şüpheli Sanal Makineler;
  $\{M_4\}$
- Güvenli Sanal Makineler;
  $\{M_1, M_2, M_3\}$

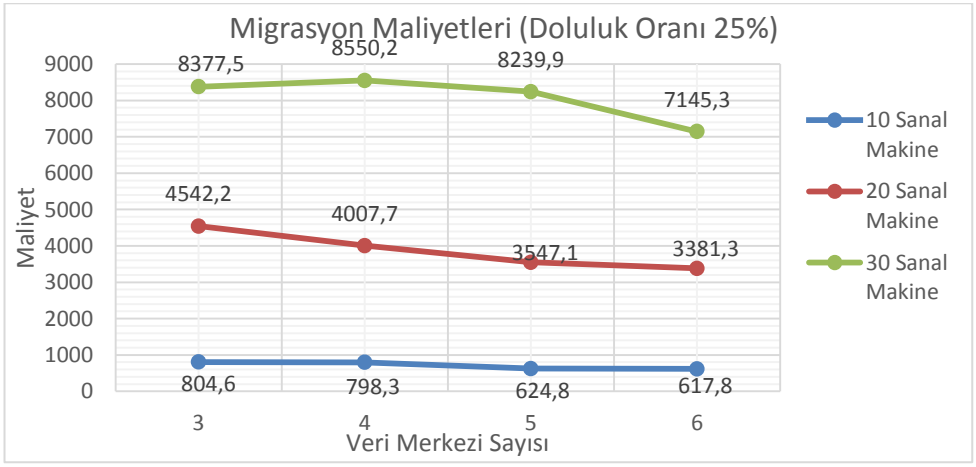
Amsterdam, Milan, Berlin ve Zurich için sanal makine kapasiteleri 5 olarak ve doluluk oranları ise %50(Aktif 3 sanal makine) olarak belirlenmiştir. Yani, bu veri merkezlerine sadece 2 sanal makine tahliyesi yapılabilmektedir.

Kodlaması yapılan tahliye modeli bu optimizasyon testini 1.4 saniyede başarıyla tamamlamıştır. Test sonucunda $\{M_1, M_2\}$ güvenli sanal makineler 9 numaralı Amsterdam veri merkezine, M_3 sanal makinesi ise 7 numaralı Berlin veri merkezine başarıyla migrasyonu (tahliyesi) yapılmıştır. $\{M_4\}$ sanal makinesi ise inceleme için 4 nolu Zurich veri merkezindeki denetim merkezine alınmıştır. Bu test sonucunda taşınması gereken sanal makineler istenilen veri merkezlerine maliyeti minimize ederek migrasyonu sağlanmıştır. Şüpheli sanal makineler denetim merkezine alınması noktasında bir incelemeden geçirilecektir ve gerekli ise karantinaya alınır ya da güvenli veri merkezlerine migrasyon edilecektir.

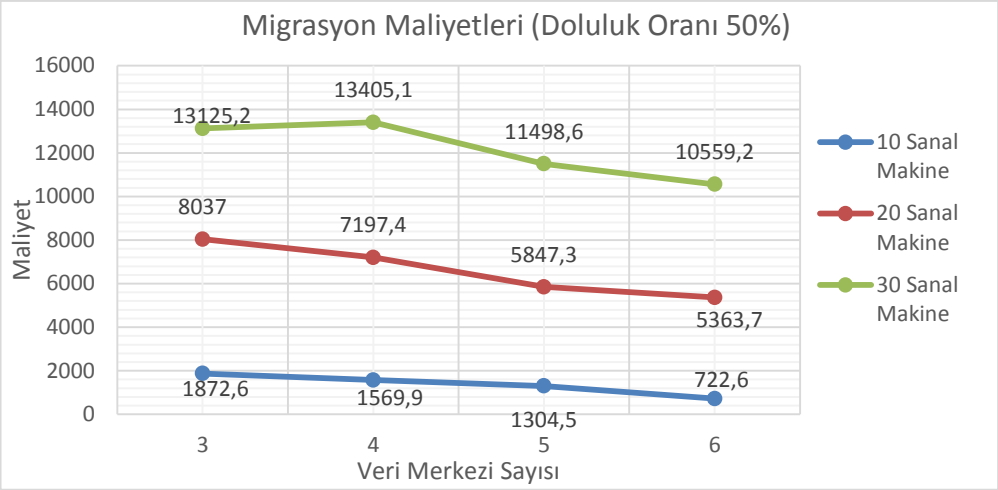
BÖLÜM 4. SONUÇLAR

GUROBI v6.5 Api desteğiyle JAVA'da kodlanan program Intel Core i7 işlemci 8GB RAM özelliklerine sahip bir makinede, farklı senaryolar belirlenerek birden fazla güvenlik testleri ile programın güvenirliği test edilmiştir ve bu testlerin de başarılı sonuç verdiği görülmüştür.

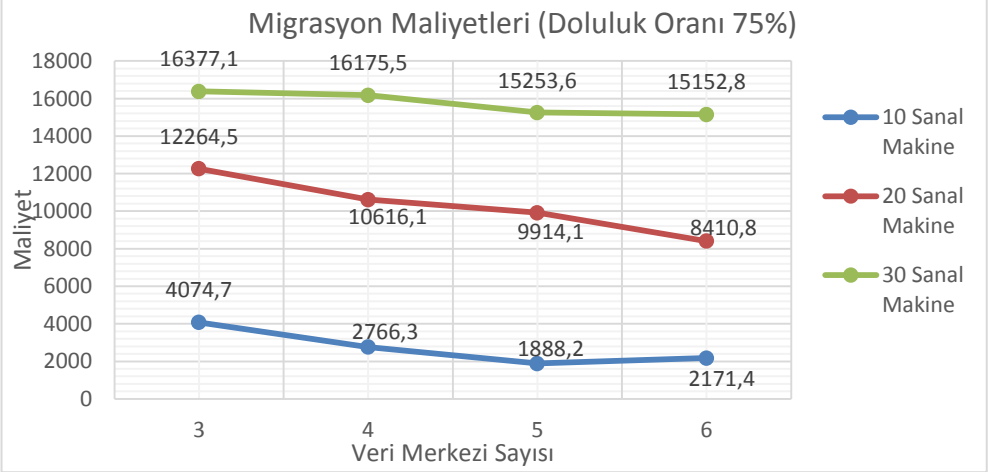
Sonuçlar toplamda 3.600 farklı senaryonun ortalaması alınarak oluşturulmuştur. Her senaryonun birbirinden farklı ve eşit olarak dağılımı için topolojiye 3, 4, 5 veya 6 farklı veri merkezi yerleştirilmiştir. Bu veri merkezlerine ise sırayla 10, 20 ve 30 sanal makine kapasitesi atanmıştır. Her bir veri merkezi sayısı için rasgele 100 farklı dağılım yapılmıştır. Veri merkezlerinde barınan toplam sanal makine sayıları ise %25, %50 veya %75 doluluk oranları sırayla seçilmiştir. Fiber yollardaki dalga boyu kapasiteleri ortalama 15 kanal olarak ve taşınma maliyetleri ise düğümler arası mesafe oranında temel alınmıştır. Saldırıya uğrayan veri merkezindeki herhangi bir sanal makinenin ise %20 olasılıkla enfekte, %30 olasılıkla şüpheli ve %50 olasılıkla güvenli olduğu kabul edilmiştir. Şüpheli paketlerin ise %60 olasılıkla enfekte, %40 olasılıkla ise güvenli olduğu kabul edilmiştir.



Şekil 4.1. Migrasyon Maliyetleri (Doluluk Oranı %25)



Şekil 4.2. Migrasyon Maliyetleri (Doluluk Oranı %50)

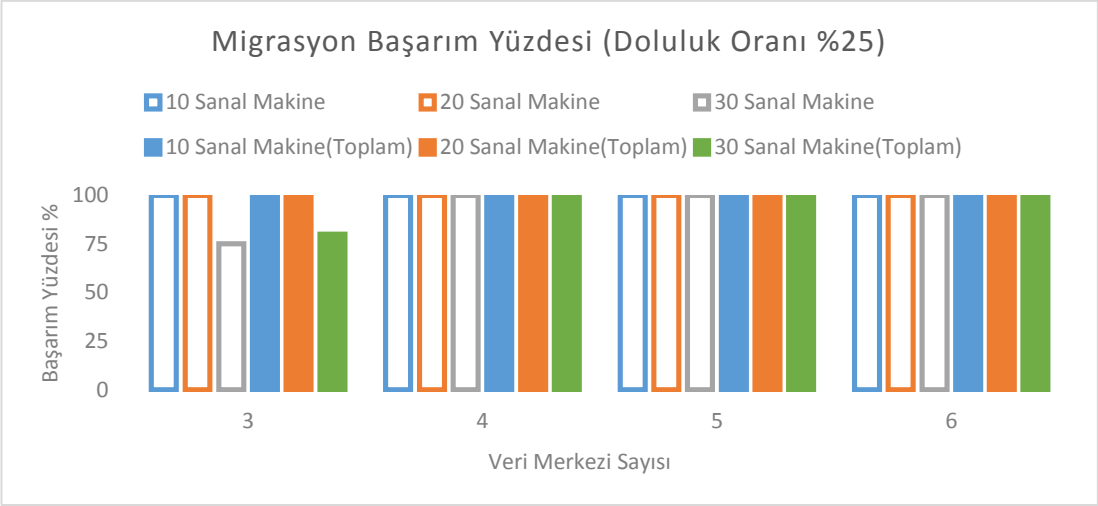


Şekil 4.3. Migrasyon Maliyetleri (Doluluk Oranı %75)

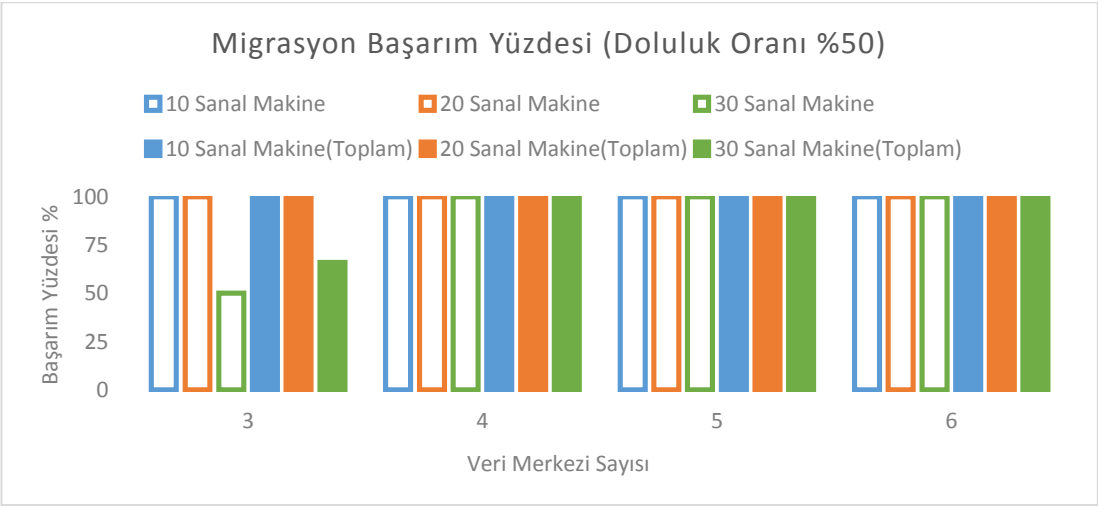
Şekil 4.1., Şekil 4.2. ve Şekil 4.3.'de veri merkezlerinin sırasıyla %25, %50 ve %75 doluluk oranında olası bir saldırıdaki sanal makinelerin tahliyesi için gerekli maliyetlerin sonuçları görülmektedir. Bu grafiklerdeki maliyet sonuçları, her bir durumdaki migrasyon edilen sanal makinelerin migrasyon mesafeleri baz alınarak hesaplanmıştır. Bu hesaplamayı bize ise amaç fonksiyonundaki migrasyon edilen sanal makinenin maliyetini minimize eden $\sum_{s\in D}\sum_{d\in D}\sum_{m\in M_d} X_d\, Lc_{s,d}^{r,m}$ formülü vermektedir. Buradaki söz konusu maliyetlerin düşük olmasının modele sağlayacağı en temel fayda, migrasyon yapılacak mesafenin küçük olması ile aktarımın çok hızlı bir şekilde ve çok kısa sürede gerçekleşecek olmasıdır.

Bu sonuçlara göre sanal makine migrasyonu yapılabilecek veri merkezi sayısının artması ile maliyetlerin azaldığı görülmektedir. Bu durumun ana sebebi migrasyon

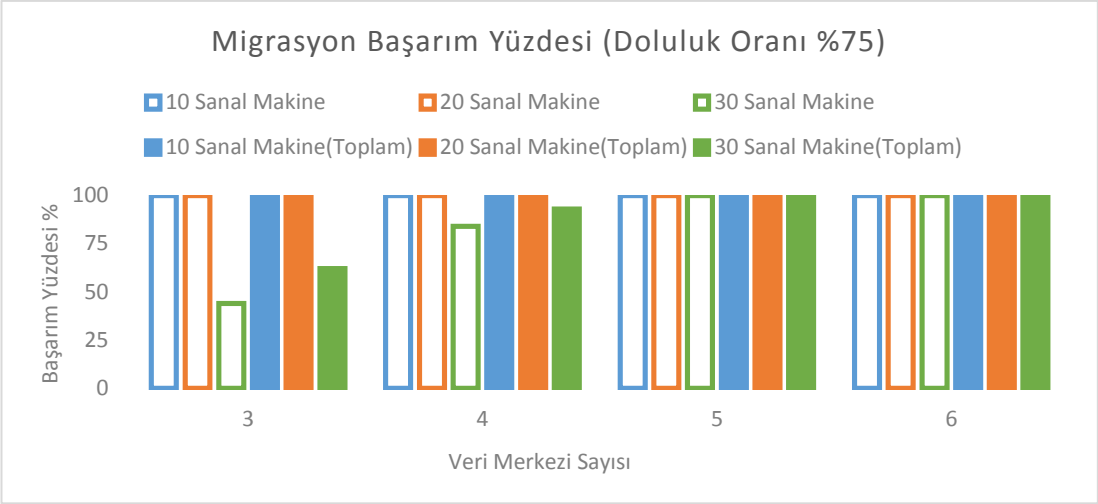
maliyeti uygun olan veri merkezlerinin bulunma olasılığının fazla olmasıdır. Ayrıca optimizasyon sonuçları maliyetlerin veri merkezlerinin doluluk oranları ile doğru, veri merkezi sayıları ile ters orantılı olduğunu göstermektedir. Örneğin, %75 doluluk oranında ve 30 sanal makine kapasite ve 3 veri merkezi olması durumunda hem kapasite yetersizliğinden hem de veri merkezi sayısının az olmasından dolayı maliyetin diğer doluluk oranlarındaki aynı durumda olan maliyetlere göre en yüksek olduğu görülmüştür. Doluluk oranları arttıkça maliyetinde buna paralel olarak artacağı sonuçlar ile desteklenmiştir.



Şekil 4.4. Migrasyon Başarım Yüzdesi (Doluluk Oranı %25)



Şekil 4.5. Migrasyon Başarım Yüzdesi (Doluluk Oranı %50)



Şekil 4.6. Migrasyon Başarım Yüzdesi (Doluluk Oranı %75)

Şekil 4.4., Şekil 4.5. ve Şekil 4.6.'da şüpheli sanal makinelerin saldırı denetim merkezlerine migrasyonun başarım yüzdeleri ve tüm migrasyon olması gereken sanal makinelerin başarım yüzdeleri verilmiştir. Bu grafikte grafik sütunlarının içi boş olanlar şüpheli sanal makineleri, içi dolu sütunlar ise tüm sanal makineleri temsil etmektedir. Bu oranlar incelediğinde optimizasyonun farklı veri merkezi sayılarında ve farklı sanal makine sayılarında bile %100'e yakın bir başarım sağladığı görülmektedir. Şekil 4.8.'de 30 sanal makine kapasitesine sahip 3 veri merkezinde %75 doluluk oranında başarım yüzdesinin %50'nin altına düştüğü tespit edilmiştir. Bu bağlamda 11 düğümlü bir veri merkezi topolojisinde başarımın yüksek olması için yani olası bir siber tehditte zararı minimize etmek adına anlaşmalı toplam veri merkezi sayısının en az 4 olması gerektiği söylenebilir.

BÖLÜM 5. SONUÇ VE DEĞERLENDİRME

Bulut bilişimde güvenliği bir bütün olarak ele aldığımızda gerçekleşebilecek saldırılara karşı tasarlanmış çok sayıda saldırı tespit sistemleri mevcuttur. Bu sistemlerin eksiklerinin giderilerek geliştirilmesine rağmen teknolojiye farklı sistemlerin adapte olması nedeniyle yeni güvenlik açıkları meydana gelmektedir. Bu arka plandan hareketle yapılan literatür araştırması sonucunda daha önce yapılan çalışmalarda savunma amaçlı birçok yazılımsal veya donanımsal sistem önerileri sunulmuştur. Fakat buna rağmen saldırı süreç analizinin yapılması ve bununla birlikte bu süreçte veri merkezlerinin saldırılara karşı hasarsız, kayıpsız ve hizmet kesintisi yaşamaması için veri merkezlerindeki sanal makinelerin kısa sürede başka bir güvenli lokasyona tahliye yöntemleri ile ilgili bir çalışma bulunmamaktadır. Bu bağlamda saldırı öncesinde fiber optik ağ üzerinden tahliye yollarının matematiksel model oluşturularak kurulması ve en güncel migrasyon teknikleri ile bir model oluşturulması çalışmanın özgün yanını oluşturmaktadır. Ayrıca bulut bilişim altyapısının daha güvenilir hale getirilmesi ve bulut bilişim sağlayıcılarının kullanıcılarına minimum risk üzerinden hizmet taahhüt edebilecek bir teknolojiye sahip olabilecek olması ticari yönden gücünü göstermektedir. Bu tür bir tahliye yöntemi birkaç çalışmada afet senaryoları için ortaya konulmuşsa da siber saldırıların kendilerine has özellikleri düşünüldüğünde ortaya koyduğumuz problemi diğer tahliye problemlerinden farklı bir noktaya taşımaktadır. Bu çalışmanın diğer bir özgün yanı ise bulut bilişim sağlayıcılarının tehdit süreçlerinde tahliye edilecek hedef makineleri satın almak yerine kiralama veya farklı antlaşmalar üzerinden farklı sağlayıcılar ile iş ortaklığına gidebilmelerine imkân sağlayacak bir acil durum platformunun oluşmasına katkı sağlayacak olmasıdır.

Bu çalışmada problemin matematiksel olarak modellemesi yapılmış olup ve bu modelleme Intel Core i7 işlemci 8GB RAM özelliklerine sahip bir makinede JAVA'da GUROBI Api desteği ile kodlanmış ve toplamda 3.600 farklı senaryo

durumu hesaplanarak her grubun ortalaması alınarak sonuçlar oluşturulmuştur. Çözümün ölçeklenebilir olması adına ise yapılan test sonuçlarının maliyet analizi yapılmıştır ve başarım oranları hesaplanmıştır. Bu sonuçlar çerçevesinde olası bir siber tehdidine karşı oluşturulacak bu modelde birbirleriyle anlaşmalı veri merkezi sayısının fazla olması zararı ve migrasyon maliyetlerini minimize etmek adına temel etken olacaktır.

Gerçekleştirilen bu modelde, tahliye işlemleri dalga boyu kapasiteleri uygun fiber yolları seçilerek, maliyeti en az rotalar belirlenmiştir. Bu rotalar üzerinden sanal makinelerin Enhanced Vmotion veya gelecekte geliştirilmesi öngörülen en gelişmiş ve en hızlı migrasyon teknikleri ile tahliye edilecek olması, siber saldırılara karşı savunma modeli olarak gerçekleştirdiğimiz bu çalışmanın gücünü artıracaktır.

KAYNAKLAR

[1] T. Şardan, «Siber saldırıya karşı 372 SOME,» 26.01.2016. http://www.memurlar.net/haber/560324/. , Erişim Tarihi: 22 04 2016.

[2] S. Ferdousi, M. F. Habib, M. Tornatore, B. Mukherjee «Rapid Data Evacuation for Large-Scale Disasters in Optical Cloud Networks,» *Optical Fiber Communications Conference and Exhibition (OFC),1-3.*, 2015.

[3] M. Liu, H. Gong, Y. Wen, G. Chen, J. Cao, «The Last Minute: Efficient Data Evacuation Strategy for Sensor Networks in Post-Disaster Applications,» *Proc. IEEE INFOCOM,*, Shanghai, 2011.

[4] T. Fujiwara, H. Makie, T. Watanabe «A Framework for Data Collection System with Sensor Networks in Disaster Circumstances,» *Proc. of International workshop on wireless Ad-hoc networking (lWW AN)*, 2004.

[5] J. Szefer, P. Jamkhedkar, Y. Chen, R. B. Lee «Physical Attack Protection with Human-Secure Virtualization in Data Centers,» *DependableSystemsand Networks Workshops (DSN-W), 2012 IEEE/IFIP 42nd International Conference on, 1 -6*, 2012.

[6] J. Szefer, E. Keller, R.B., Lee, Rexford, J. «Eliminating the Hypervisor Attack Surface for a More Secure Cloud,» *Proceedings of the 18th ACM Conference on Computer and Communications Security, 401-412*, 2011.

[7] J. X. Y. Xiujie Feng, *A performance study of live VM migration technologies: VMotion vs XenMotion. Shanghai Jiao Tong University*, Shanghai: State Key Laboratory of Advanced Optical Communication Systems and Networks, 2011.

[8] X. v. Y. XiujieFeng, «An acceleration system for long distance live migration of virtual machine,» *Optical Internet (COIN), 2012 10th International Conference on,10-11*, 2012.

[9] A. Celesti, A. Salici, M. Villari, A. Puliafito «A Remote Attestation Approach for a Secure Virtual Machine Migration in Federated Cloud Environments,» *Network Cloud Computing and Applications (NCCA), 2011 First International Symposium on. 21-23 Nov. 2011*, 2011.

[10] R. Miller, «Amazon Adding Cloud Capacity in Northern Virginia,» Data Center Knowledge,01.15.2013.http://www.datacenterknowledge.com/archives/2013/01/15/amazon-to-add-capacity-to-us-east-region/. , Erişim Tarihi: 12.04.2016.

[11] A. Günel, *Üniversitelere Yönelik Yeni Bir Veri Merkezi Tasarımı ve Uygulaması,* Bilecik Şeyh Edebali Üniversitesi ,Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans Tezi, 2014.

[12] H. Yehia ve M. Khalil , *Data center resilience assessment : storage,networking and security,* The University of Louisville's Institutional Repository, 2011.

[13] Google Inc., «Google Data Center,» Google, http://www.google.com/about/datacenters/. , Erişim Tarihi: 02.04.2016.

[14] A. Erduran, «Veri Merkezi Sınıflandırmaları,» 01.12.2013. http://www.mshowto.org/veri-merkezi-siniflandirmalari.html. , Erişim Tarihi: 01.03.2016.

[15] «Veri Merkezlerinin Sahip Olması Gereken Özellikler,» http://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/veri-merkezlerinin-sahip-olmasi-gereken-ozellikler.html. , Erişim Tarihi: 24.03.2016.

[16] Vikipedi, «Veri Merkezi,» Vikipedi, https://tr.wikipedia.org/wiki/Veri_merkezi. , Erişim Tarihi: 02.04.2016.

[17] Y. Vural ve Ş. Sağıroğlu, «Kurumsal Bilgi Güvenliği ve Standartları. Gazi Üniversitesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü,» *Gazi Üniv. Müh. Mim. Fak. Der.,* cilt 23, no. 2, pp. 507-522, 2008.

[18] N. Barret, «Penetration testing and social engineering: Hacking the weakest link, 8(4):56-58,» Information Security Technical Report, 2003.

[19] J. Allen, *The CERT® Guide to System and Network Security Practices. Carnegie Mellon University, Software Engineering Institute, Networked Systems Survivability Program, CERT Coordination Center,* 2001.

[20] S. Kalman, «Web Security Field Guide,» *Cisco Press,* Indianapolis, 2003, pp. 36,37.

[21] Y. Vural ve Ş. Sağıroğlu, «Kurumsal Bilgi Güvenliğinde Güvenlik Testleri» *Gazi Üniv. Müh. Mim. Fak. Der.,* cilt 26, no. 1, pp. 89-103, 2011.

[22] Y. Vural ve Ş. Sağıroğlu, *"Kurumsal Bilgi Güvenliği ve Sızma. Yüksek Lisans Tezi, Gazi Üniversitesi,,* cilt 26, Ankara, 2007, pp. 89-103.

[23] Vikipedi, «Bulut bilişim,» 16.04.2016. https://tr.wikipedia.org/wiki/Bulut_bilisim. , Erişim Tarihi: 02 04 2016.

[24] International Trade Administration, «2016 Top Markets Report,» 01.04.2016. http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf. , Erişim Tarihi: 20.04.2016.

[25] E. Gülyaşar, «Türkiye'de kamu kurumları buluta geçiyor,» BtHaber, 24 11 2014,http://www.bthaber.com/kamuda-verimlilik-icin-bulut-bilisim/turkiye'de-kamu-kurumlari-buluta-geciyor/1/13860. , Erişim Tarihi: 22.04.2016.

[26] O. Şanlı, «Bulut Bilişim. PayDeg Bilgi İşlem Programlama Hizmetleri,» *MCT,MCAS,MCTS*, İstanbul.

[27] O. Sevli, *Bulut Bilişim Ve Eğitim Alanında Örnek Bir Uygulama. Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Yüksek Lisans Tezi*, Isparta, 2011.

[28] H. Yüksel, Bulut Bilişim El Kitabı, Ocak 2012.

[29] Y. D. D. M. T. Sarıtaş, «Yenilikçi Teknolojiler: Bulut Teknolojisi» *Eğitim ve Öğretim Araştırmaları Dergisi,* cilt 2, no. 3, pp. 2146-9199, 2013.

[30] K. Weins, «Cloud Computing Trends: 2015 State of the Cloud Survey,» Right Scale, 15.02.2015.http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2015-state-cloud-survey#Hybrid. , Erişim Tarihi: 04.04.2016.

[31] G. Canbek ve Ş. Sağıroğlu, «Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme. Gazi Üniversitesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü,» *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi,* cilt 1, no. 23, pp. 1-12, 2007.

[32] P. Passeri, «February 2016 Cyber Attacks Statistics,» 26.03.2016. http://www.hackmageddon.com/2016/03/24/february-2016-cyber-attacks-statistics/. , Erişim Tarihi: 12.04.2016.

[33] A. Aykanat, «Türkiye'de Tam 50 Milyon Kişinin Kimlik Bilgileri Çalındı,» 03.04.2016. Available: http://www.webtekno.com/internet/turkiye-de-tam-50-milyon-kisinin-kimlik-bilgileri-calindi-h15929.html. , Erişim Tarihi: 12.04.2016.

[34] Statista, «Cyber crime: largest online data breaches 2007-2016,» 01 02 2016. http://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/. , Erişim Tarihi: 12.04.2016.

[35] D. M. Ajey Singh, «Overview of Attacks on CloudComputing,» *International Journal of Engineering and Innovative Technology, Volume 1, ISSN: 2277-3754,* 2012.

[36] M. Chirag, D. Patel, B. Borisaniye, H. Patel, A. Patek ve M. Rajarajan, «A survey of intrusion detection techniques in Cloud,» *Journal of Network andComputer Applications,* no. 36, pp. 42-57, 2013.

[37] A. Chonka, Y. Xiang, W. Zhou ve A. Bonti, «Cloud security defence to protect cloud computing against HTTP-DoS. School of Information Technology, Deakin University, Australia,» *Journal of Network and Computer Applications,* no. 34, p. 1097–1107, 2011.

[38] F. Şölen, «Sanallaştırma Nedir? Neden Sanallaştırma?,» 14.08.2009. http://www.fatihsolen.com/neden-sanallastirma-sanallastirma-nedir/. , Erişim Tarihi: 12.04.2016.

[39] M. Parlakyiğit, «Hypervisor Nedir? ve Hypervisor Türleri,» Microsoft, 13.03.2014. http://social.technet.microsoft.com/wiki/contents/articles/17648.hypervisor-nedir-ve-hypervisor-turleri-tr-tr.aspx. , Erişim Tarihi: 12.04.2016.

[40] J. Szefer, E. Keller, R. B. Lee ve J. Rexford, «Eliminating the Hypervisor Attack Surface. Princeton University,» *18th ACM conference*, 2011.

[41] S. Subashini ve V. Kavitha, «A survey on security issues in service delivery models of cloud computing,» *Journal of Network and Computer Applications. Anna University Tirunelveli,* no. 34, pp. 1-11, 2011.

[42] Wikipedia, «Optical Network,» Wikipedia, 16.01.2016. https://en.wikipedia.org/wiki/Optical_networking. , Erişim Tarihi: 04.04.2016.

[43] M. A. A. Z. Özgür Can Turna, «Pasif Optik Erişim Ağlarının Gelişimi. İstanbul Üniversitesi, Bilgisayar Mühendisliği Bölümü,» *Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri*, Şanlıurfa, 2009.

[44] University of Massachusetts Lowell, «NSF Service-Oriented Optical Networks (SOON) Project,» University of Massachusetts Lowell, http://faculty.uml.edu/vinod_vokkarane/soon/index.html. , Erişim Tarihi: 12.04.2016.

[45] VMware, «VmWare Documentation Center,» https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vcenterhost.doc%2FGUID-FE2B516E-7366-4978-B75C-64BF0AC676EB.html.

[46] Vmware, «vSphere and vSphere with Operations Management,» Vmware, https://www.vmware.com/products/vsphere/features/vmotion. , Erişim Tarihi: 14.05.2016.

[47] Türkiye Standartlar Enstitüsü, «Türkiye Standartlar Enstitüsü Veri Merkezi Altyapısı Standart Taslağı,» https://www.tse.org.tr/upload/tr/dosya/icerikyonetimi/2222/17032015164319-3.pdf. , Erişim Tarihi: 02.04.2016.

[48] EOS Elektronik, «Data Center Standartları,» 05.12.2011. http://www.eoselektronik.com.tr/data-center-standartlari-211/. , Erişim Tarihi: 20.03.2016.

[49] G. Canbek ve Ş. Sağıroğlu, «Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine. Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü,» *Politeknik Dergisi,* cilt 9, no. 3, pp. 165-174, 2006.

[50] International Organization for Standardization, *Information technology, Code of practice for information. ISO-17799,* 2000.

[51] J. Brodkin, «Gartner: Seven cloud-computing security risks,» 2 07 2008. http://www.networkworld.com/article/2281535/data-center/gartner--seven-cloud-computing-security-risks.html. , Erişim Tarihi: 13.04.2016.

[52] V. Ugale, «Cloud Computing,» 9.10.2015. http://ohioerc.org/?page_id=187. , Erişim Tarihi: 04.04.2016.

ÖZGEÇMİŞ

Emre Karakoç, 21.03.1989'da Sivas'ta doğdu. İlk, orta ve lise eğitimini Sivas'ta tamamladı. 2007 yılında Sivas Selçuk Anadolu Lisesi'nden mezun oldu ve yine aynı yıl Sakarya Üniversitesi Bilgisayar Mühendisliği Bölümünü kazandı ve 2012 yılında mezun oldu. 2012 yılında İnotek Mühendislik adlı firmada Ar-Ge Mühendisi olarak göreve başladı. Burada 1 seneye yakın çalıştıktan sonra 2013 yılında İstanbul'da Tegsoft firmasında Yazılım Mühendisi olarak göreve başladı. Bu firmada da yaklaşık 1 sene çalıştıktan sonra 2014 yılında Berrak Sistem adlı Ar-Ge firmasında proje yöneticiliği olarak göreve başladı ve halen bu firmada fiili olarak görevine devam etmektedir.