

T.C.

**GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ**

**OYUN TEORİSİ KULLANILARAK BULUT
BİLİŞİM İÇİN ÖLÇEKLENDİRİLEBİLİR
GÜVENLİK DEĞERLENDİRMESİ**

**Evrin FURUNCU
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**

GEBZE

2012

T.C.

**GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ**

**OYUN TEORİSİ KULLANILARAK BULUT
BİLİŞİM İÇİN ÖLÇEKLENDİRİLEBİLİR
GÜVENLİK DEĞERLENDİRMESİ**

**Evrin FURUNCU
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**

**DANIŞMANI
Prof. Dr. İbrahim SOĞUKPINAR**

GEBZE

2012



YÜKSEK LİSANS TEZİ JÜRİ ONAY SAYFASI

G.Y.T.E. Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 04/10/2012 tarih ve 2012/37 sayılı kararıyla oluşturulan jüri tarafından 08/10/2012 tarihinde tez savunma sınavı yapılan Evrim FURUNCU'nun tez çalışması Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE

(TEZ DANIŞMANI) : Prof. Dr. İbrahim SOĞUKPINAR

ÜYE

: Doç. Dr. Hacı Ali MANTAR

ÜYE

: Yrd. Doç. Dr. S. Süer ERDEM

ONAY

G.Y.T.E. Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun/...../20... tarih ve/..... sayılı kararı.

İMZA/MÜHÜR

ÖZET

TEZİM BAŞLIĞI: OYUN TEORİSİ KULLANILARAK BULUT BİLİŞİM İÇİN ÖLÇEKLENDİRİLEBİLİR GÜVENLİK DEĞERLENDİRMESİ

YAZAR ADI: EVRİM FURUNCU

“Bulut Bilişim” bilgisayar kaynaklarının servis olarak temin edilmesidir. Bu teknolojik gelişme esnek bilgi teknolojilerinin kullanımını verimliliğine göre uygun bir fiyata sunmakla beraber, aynı zamanda kullanıldığı kadar harcama yolun ile öne çıkmaktadır. Bulut bilişimin organizasyonlar ve kişiler tarafından kullanımı her geçen gün artmaktadır. Bulut bilişim üzerinde oluşabilecek güvenlik açıklıkları, güvenlik sorunları ve riskler normal bir bilgi teknolojisi sisteminden farklı olarak, aynı altyapıyı birden fazla organizasyonun ve kişinin kullanıldığı düşünüldüğünde önemli bir sorun halini almaktadır.

Bu çalışmada günümüz bulut bilişim yapısı üzerinde güvenlik değerlendirilmesi konusu ele alınmıştır. Mevcut güvenlik değerlendirme yöntemlerinin bulut bilişim üzerinde uygulanmasındaki eksik noktalar gösterilerek, bulut bilişim hizmet modellerine göre ölçeklendirilebilir bir güvenlik değerlendirme yöntemi geliştirilmiştir. Bulut bilişim hizmet modellerinde uygulanan güvenlik, kullanılan altyapı nedeniyle birbirleri arasında farklılıkları göstermektedir. Bir modeldeki güvenlik sorumluluğu diğer modellerde farklı kişi veya kuruluşlara aktarılmakta ve bu aktarım yüzünden kimin hangi güvenlikten sorumlu olduğuyla alakalı bir karmaşa yaşanmaktadır. Bunun dışında bulut bilişim sistemi içindeki her varlık hizmet modeline göre farklı güvenlik önlemi gerektirebilmektedir. Bu husus önemsiz bilgilerin yüksek güvenlik seviyesi ile saklanmasına neden olmakta ve bulut sağlayıcıyı gereksiz masraflara sokmaktadır.

Çalışmada oyun teorisi kullanılarak bulut bilişim için ölçeklendirilebilir güvenlik değerlendirilmesi yöntemi sunulmuştur. Oyun teorisi kullanılarak sistem üzerindeki herhangi bir riskin sistemi kiralayan kişinin mi yoksa bulut bilişim sağlayıcının mı çözmesi gerektiği değerlendirilmektedir.

SUMMARY

**THESIS TITLE: SCALABLE RISK ASSESSMENT SYSTEM FOR
CLOUD COMPUTING USING GAME THEORY**

AUTHOR: EVRİM FURUNCU

“Cloud computing” is the use of computing resources that are delivered as a service. This technological development stands out by offering flexible information technology (IT) usage in a cost efficient and pay-what-you-use way. Organizational and personal adaptation of cloud computing is increasing day by day. Vulnerabilities, security problems and risks in cloud computing differs from the traditional IT because unlike normal IT, same infrastructure that is used by different organizations and people poses an important risk.

In this work, risk assessment on cloud computing is discussed. By showing current cloud computing risk assessments’ missing points, a new method for cloud risk assessment based on cloud computing service models is developed. The security implemented in each service model is different than other models because of the need for different infrastructure elements for each service model. The security responsibility for an asset in a model may be transferred to other persons or entities in another model. Each asset depending on the deployment or service model may need different security level than other assets. This state may cause unimportant information to have more security then needed and results in unnecessary expense.

Current systems generally focus on static risk assessments which require more time to do and generally do not produce good results for cloud computing systems. In this work, a scalable security risk assessment has been proposed as a solution for this problem. This solution is presented by using game theory. It can be evaluated whether the risk in the system should be fixed by cloud provider or tenant of the system using game theory.

TEŞEKKÜR

Öncelikle, yüksek lisans eğitimim süresince bilgi ve tecrübeleri ile bana yol gösteren ve destek olan değerli hocam Prof. Dr. İbrahim Soğukpınar'a,

Öğrenim hayatımın her aşamasında bana emek veren tüm eğitimcilere,

İş hayatım boyunca bana yardımcı olan ve destek veren araştırma görevlisi arkadaşlarıma,

Oda arkadaşlarım olan Arş. Gör. Alper Uğur ve Arş. Gör. Arzu Görgülü Kakışım'a verdikleri destekten,

Ve her zaman, bana her konuda destek ve yardımcı olan çalışan anneme ve babama, sonsuz ve içten teşekkürlerimi sunuyorum.

İÇİNDEKİLER DİZİNİ

ÖZET	iv
SUMMARY	v
TEŞEKKÜR	vi
İÇİNDEKİLER DİZİNİ	vii
SİMGELER VE KISALTMALAR DİZİNİ	ix
ŞEKİLLER DİZİNİ	x
TABLOLAR DİZİNİ	xi
1. GİRİŞ	1
2. BULUT BİLİŞİM GÜVENLİĞİ VE ALANDAKİ ÇALIŞMALAR	3
2.1. BULUT BİLİŞİM	3
2.1.1. BULUT BİLİŞİM NEDİR?	3
2.1.2. BULUT BİLİŞİM SERVİS MODELLERİ	7
2.1.3. BULUT BİLİŞİM KURULUM MODELLERİ	9
2.1.3.1. GENEL BULUT	9
2.1.3.2. ÖZEL BULUT	9
2.1.3.3. ORTAKLIK BULUTU	9
2.1.3.4. MELEZ BULUT	9
2.1.4. BULUT BİLİŞİMİN AVANTAJLARI	10
2.1.5. BULUT BİLİŞİMİN DEZAVANTAJLARI	11
2.1.6. BULUT BİLİŞİMİN GÜVENLİK ANALİZİ	11
2.1.6.1. VERİ GÜVENLİLİĞİ VE GİZLİLİĞİ	12
2.1.6.2. ERİŞİLEBİLİRLİK	13
2.1.6.3. HİZMET BAĞIMLILIĞI	13
2.1.6.4. KİMLİK ERİŞİMİ VE YÖNETİMİ	14
2.1.6.5. UYGULAMA GÜVENLİĞİ	15

2.1.6.6. YASAL UYUMLULUK	15
2.1.7. ÖLÇEKLENDİRİLEBİLİR BULUT BİLİŞİM GÜVENLİĞİ	16
2.2. OYUN TEORİSİ	20
2.2.1. OYUN TEORİSİ NEDİR?	20
2.2.2. OYUN TEORİSİ GÜVENLİK MODELLEMESİ	22
2.2.3. OYUN TEORİSİNİN GÜVENLİK ALANINDA KULLANIMI	24
2.2.4. OYUN TEORİSİNİ KULLANAN BİR GÜVENLİK ÖRNEĞİ	24
2.3. BULUT BİLİŞİM GÜVENLİĞİ İLE İLGİLİ ÇALIŞMALAR	26
3. OYUN TEORİSİ KULLANARAK BULUT BİLİŞİM RİSK DEĞERLENDİRME MODELİ	30
3.1. SALDIRI MODELLEMESİ	31
3.2. SİSTEMİN DEĞERİNİN HESAPLANMASI	32
3.3. RİSKLERİN KARŞILAŞTIRILMASI	34
3.4. KAZANÇ TABLOSUNUN HESAPLANMASI	34
3.5. SAVUNMANIN KAZANCI	35
3.6. SAVUNMANIN MALİYETİ	36
3.7. SALDIRGANIN KAZANCI	36
3.8. SAVUNMANIN MALİYETİ	37
4. UYGULAMA ÖRNEĞİ VE DEĞERLENDİRME	38
4.1. RİSK KARŞILAŞTIRMA	38
4.2. RİSK OYUNU	40
5. SONUÇ VE ÖNERİLER	43
KAYNAKLAR	45
ÖZGEÇMİŞ	51

SİMGELER VE KISALTMALAR DİZİNİ

BBGOTM	: Bulut Bilişim Güvenliğinin Oyun Teorisi Modeli
BT	: Bilgi Teknolojileri
GBE	: Gizlilik, Bütünlük, Elde edilebilirlik
HSA	: Hizmet Seviye Anlaşması (Service Level Agreement)
SETI	: Dünya Dışı Akıllı Yaşam Araştırması
SoA	: Servis olarak Yazılım
SoaA	: Servis olarak Ağ
SoDA	: Servis olarak Depolama Alanı
SoM	: Servis olarak Masaüstü (Masaüstü Sanallaştırılması)
SoP	: Servis olarak Platform
SoV	: Servis olarak Veri
SoY	: Servis olarak Yazılım
VT	: Veri tabanı

ŞEKİLLER DİZİNİ

<u>Sekil</u>	<u>Sayfa</u>
2.1 - Bulut Bilişim Temelleri	4
2.2 - Bulut Bilişimin Mantıksal Şeması	5
2.3 - Bulut Hizmet Modelleri ve Kullanıcıları	7
2.4 - Bulut Bilişim Kurulum Modelleri	10
2.5 - Bulut Bilişim Güvenlik Karmaşıklığı	12
2.6 – Farklı Servis Modellerinin Sorumlu Olduğu Kısımlar	17
2.7 - Servis olarak Yazılım Güvenlik Yığını	18
2.8 - Bazı Örnek Bulut Hizmetlerinde Sorumlu Olunan Kısımlar	19
2.9 - Bir Bulut Oyun Teorisi Güvenlik Örneği	25

TABLÖLAR DİZİNİ

<u>Tablo</u>	<u>Sayfa</u>
2.1 - Bulut Bilişim Güvenlik Gereksinimleri	16
2.2 - Tutsak İkilemi Çözüm Matrisi	20
2.3 - Polis ve Saldırgan Arasında Geçen Güvenlik Oyunu	23
3.1 - Örnek Saldırı Sınıflandırması	32
3.2 - Örnek Savunma Sınıflandırması	32
3.3 - Savunmanın Kazancı	35
3.4 - Savunmanın Maliyeti	36
3.5 - Saldırganın Kazancı	37
3.6 - Saldırganın Maliyeti	37
4.1 - Farklı Servis Modellerindeki Sunucuların Varlık Değerleri	38
4.2 - Risklerin Hesaplanan Etkisi	39
4.3 - SoY Veri Tabanı Sunucusu Çözüm Matrisi	40
4.4 - SoA Veri Tabanı Sunucusu Çözüm Matrisi	41

1. GİRİŞ

Bilgi, elektronik veya yazılı halde saklanabilen, başkalarına iletilebilen, görüntülü, yazılı veya sözlü gibi çeşit formatlarda olabilen ve gerekli şekilde korunması gereken bir varlıktır. Organizasyonlar için bilgi, diğer iş değerleri kadar bir öneme sahip olduğundan uygun şekilde korunmaya ihtiyaç duyar. Bilgi güvenliği; organizasyondaki işlerin devamlılığını sağlanması, meydana gelebilecek iş kaybının azaltılması, yapılacak yatırımlardan gelecek faydanın artırılması için geniş çaplı tehditlerden, gizlilik, bütünlük ve erişilebilirlik güvenlik özellikleri dikkate alınarak bilgiyi korumaya çalışır. Her geçen gün bilgi üzerine daha fazla karmaşık ve zararlı saldırılar gerçekleştirilmektedir.

Bulut bilişim, bilgisayar kaynaklarının bir ağ üzerinden servis olarak sunulmasıdır. Bulut bilişimin birden fazla organizasyon veya kişinin aynı altyapıyı kullanmasıyla oluşması, sistemin verimli olarak kullanılmasını sağlamaktadır. Bu şekilde ucuzlayan altyapı maliyeti, kiralanan bilgisayar kaynaklarının fiyatlarına yansımaktadır. Bulut bilişime bel bağlayarak, işletmeler bilgisayar kaynakları maliyetlerinde tasarruf, esneklik ve seçim elde edebilirler. Talep üzerine kapasite ekleyerek, işletmeler bulut bilişimi kendi altyapılarını genişletmek için kullanabilirler. Bulut bilişimde işlenen veya saklanan bilginin güvenliği, bulut bilişim yaygınlaştıkça giderek önem kazanmaktadır. Bunun temel nedeni günümüz bilgi teknolojileri (BT) güvenlik yapısının, bulut bilişim ile aynı olmamasından kaynaklanmaktadır. Birden fazla kişi tarafından paylaşılan altyapı, dışardan gelebilecek tehditler dışında, içeriden gelebilecek tehditlere karşıda korunmasını gerektirmektedir.

Birden fazla kullanıcının ortak altyapı kullanması bulut bilişim sistemin güvenliğini önemli kılmaktadır. Bulut bilişimin hizmet modelleri olan; Servis olarak Yazılım (SoY), Servis olarak Platform (SoP) ve Servis olarak Altyapı (SoA) modellerinin her birisinde farklı hizmetler belirli bir kademeye kadar çalıştırılmaktadır. Mevcut hizmet modellerinde, ihtiyaç duyulan farklı kaynaklar nedeniyle alınan güvenlik önlemleri de farklılık göstermektedir. Güvenlik

önlemlerinin bazı hizmet modellerinde sağlayıcının tarafından alınması gerekirken, bazı hizmet modellerinde alınması zorunlu olmamakta veya hizmet modeline göre var olan güvenliğin sorumluluğu hizmet alan tarafından veya üçüncü bir şahıs/firma tarafından yapılmalıdır. Bu önlemlerin servis modellerine göre değişiklik göstermesinin yanı sıra, bulut servis sağlayıcılar ile kullanıcılar arasında yapılan hizmet seviyesi anlaşmasına (Service Level Agreement (SLA)) göre de değişebilmektedir.

Genel olarak saldırganlar zeki ve mantıklı insanlardır. Yapacakları saldırıların masraflarını ve kazançlarını göz önünde bulundururlar. Savunanlar ise saldırıyı engelleyerek zararı azaltmaya çalışmakta, fakat herhangi bir saldırı olmadığı zamanda aldıkları güvenlik önlemlerinin gereksiz bir maliyeti olmaktadır. Belirtilen özellikler bu durumun oyun teorisi tarafından modellenmesini uygun kılmaktadır. Bulut bilişimde, ağ güvenliğinde olduğu gibi, saldırganlar ve savunanlar arasında çok önemli bir oyun bağlantısı bulunmaktadır. Savunanın ideal savunma stratejisi ve saldırganın saldırı stratejileri birbirleri ile bağlılık göstermektedir.

Bu çalışmada, saldırganların ve savunanların bu özellikleri kullanılıp, yapılan saldırılar ve alınabilecek güvenlik önlemleri göz önüne alınarak saldırgan ve savunan için ideal stratejilerin belirlenebilmesi amacıyla bir model önerilmiştir. Yöntemin kullanılmasıyla ortaya çıkan, sonuca göre saldırgan veya savunanın kendi kârını artıran veya kendine en az zararı verdiren stratejiler ilgili oyuncuların önüne sunulmaktadır. Sonuçta bulut bilişim güvenlik elemanları kazançlarına ve kayıplarına göre karar vererek, gerekli güvenlik önlemlerini geliştirebileceklerdir.

Tezin organizasyonu aşağıdaki şekildedir: İkinci bölümde oyun teorisinin temelleri ve ilgili çalışmalar verilmiştir. Üçüncü bölümde önerilen oyun teorisi modeli açıklanmıştır. Dördüncü bölümde çalışmayı örneklemek için bir vaka ve analiz sunulmuştur. Sonuç bölümünde yapılan çalışma değerlendirilip, gelecekte yapılacaklar ve geliştirilmesi gereken noktalar aktarılmıştır.

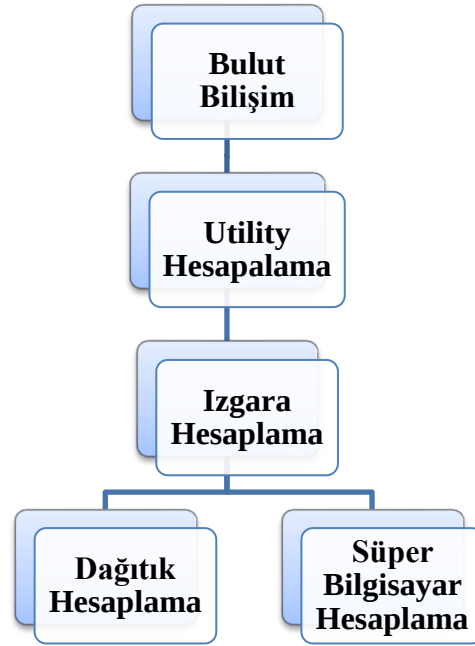
2. BULUT BİLİŞİM GÜVENLİĞİ VE İLGİLİ ÇALIŞMALAR

2.1. BULUT BİLİŞİM

2.1.1. BULUT BİLİŞİM NEDİR?

En basit tanımıyla bulut bilişim, gelişen bağlantı hızları sayesinde uzaktaki güçlü sunucuların kaynaklarının kullanılarak hesaplama veya depolama yapılmasıdır. Aslında var olan sistemler üzerinde zaten gerçekleştirilmekte olan bir durumdur. Barındırma (hosting) firmalarından bir sunucu kiralandığında, uzakta bulunan sunucu site yayınlamakta veya programların çalıştırmasında kullanmakta idi. Üniversitelerde veya çeşitli organizasyonlarda yapılan araştırmalarda, ortak bir amaca ulaşmak için, ya birden fazla var olan bilgisayarlar arasında veya büyük araştırmalar için yapılmış paralel çalışan sistemler arasında yükün dağıtılmakta idi (ızgara hesaplama veya dağıtık hesaplama (grid computing)). Dünya Dışı Akıllı Yaşam Araştırması (SETI) projesi içinde bulunana SETI@home hesaplama projesi dağıtımlı hesaplama bir örnek sayılabilir. Görüldüğü üzere aslında bulut bilişimin tanımı günümüzdeki barındırma ve dağıtık hesaplama hizmetlerinin yaptıklarını içine almaktadır.

Bulut bilişimin arkasında yatan kavram 1960 yıllarına kadar gitmektedir. John McCarthy'nin "Hesaplama bir gün bir kamu hizmeti olarak organize edilebilir" fikri bulut bilişimin temeli olarak sayılabilir. Bulut bilişim elektriğin yaygınlaştığı ilk zamanlar ile karşılaştırılmaktadır. Evler, iş yerleri ve kasabalar kendi kaynaklarından enerji üretmek ve buna bel bağlamak istemediler. Bu yüzden kendilerini elektrik üretmek ve dağıtmakla görevli olan firmaların destek sağladığı ve kontrol ettiği daha büyük bir elektrik şebekesine bağladılar. Bu bağlantı ile birlikte para ve zaman kazancı sağlamakla beraber daha büyük başarımlar ve daha güvenilir bir güç elde edildi. Bugün bulut bilişimin sahip olduğu tüm karakterler, Douglas Parkhill'in 1966 yayınladığı "The Challenge of the Computer Utility" kitabında elektrik endüstrisi ile karşılaştırılmıştır.



Şekil 2.1 - Bulut Bilişim Temelleri

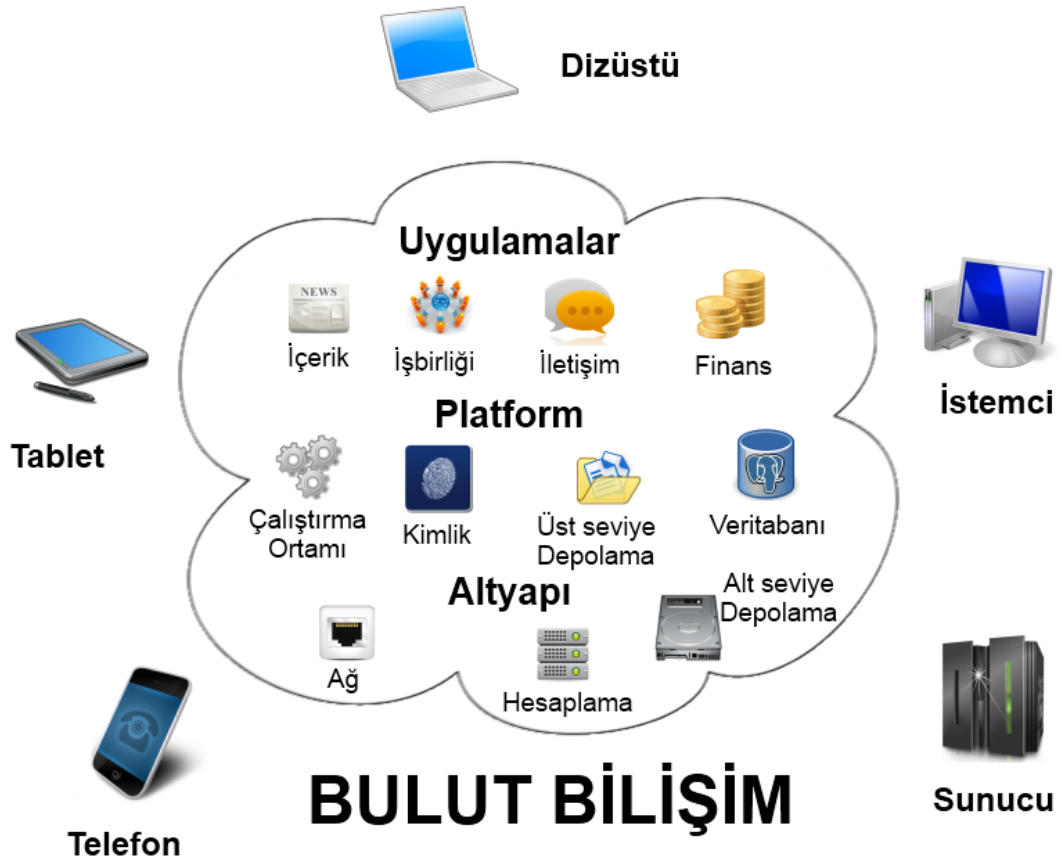
Aynı şekilde günümüzde bulut bilişim servis sağlayıcılar ve kuruluşlar için çok önemli fırsatlar temsil etmektedir. Kuruluşlar bulut bilişimi kullanarak bilgisayar kaynakları konusunda esneklik ve seçim olanaklarını artırırken aynı zamanda maliyetten tasarruf sağlamaktadırlar. Talep üzerine kapasite ekleyerek, işletmeler bulut bilişimi kendi altyapılarını genişletme kullanabilirler.

Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü'nün yayınladığı rapora göre bulut bilişim, hızlıca sağlanabilip, bırakılabilen, düşük yönetim çabası ve servis sağlayıcı etkileşimi gerektiren paylaşılan bilgisayar kaynakları havuzuna, istenilen yerden uygun bir şekilde ağ erişimi sağlayan bir modeldir [1].

Bilgiler, bulut bilişim ile Internet üzerinde hizmet veren paylaşılan sunucuların üzerinde saklanmaktadır. Aynı şekilde bu bilgiler üzerinde değişiklik bir istemcinin bu sunucuya bağlanarak bilgiyi edinmesi veya üzerinde değişiklik yapmasıyla kullanılmaktadır. Sunucu, istemci ve son zamanlarda ise uygulamaların sanallaştırılması sayesinde kaynakların daha verimli paylaşılması bulut bilişimin temellerini atmıştır. Bulut bilişimde kuruluşlar ve kişiler kullanmak istedikleri hizmeti kiralarlar veya satın alırlar. Bu hizmetin arkasında çalışan donanım ve

yazılım lisans masrafları bulut sağlayıcı tarafından karşılanmakta olup kullanıcının bu gibi sorunlarla ilgilenmesini ortadan kaldırır.

Son yıllarda internete bağlanmakta kullanılan ağlarda bant genişliği kapasitelerinin artırılması, fiber optik ve xDSL gibi geniş bant teknolojilerinin herkesin kullanabileceği mertebede fiyatlara indirilmesi bulut bilişimi yaygınlaşmasını sağlayan önemli faktörler arasındadır. Bulut bilişim üzerinden sağlanan hizmetlerin hepsinin internet üzerinden verildiği düşünüldüğünde, geniş bant gerektiren hizmetlerin (veri depolama, video yayını vb.) eskiden internet üzerinden gönderilme olanağı yok idi.



Şekil 2.2 - Bulut Bilişimin Mantıksal Şeması

Bulut bilişim kullanılması için genelde ilave bir yazılıma ihtiyaç duyulmamakta ve her şey bir internet gezgini üzerinde yapılabilmektedir. Bu şekilde istemci üzerine paket program olarak kurulan ofis programları, resim düzenleyiciler, uygulama

geliştirme programları vb. gibi araçlar internet gezginleri üzerinden istemciye sunulabilmektedir. Örneğin, son yıllarda en çok kullanılan ofis programı olan Microsoft Office muadili ve bulut üzerinden çalışan Office 365 hizmetini buna örnek olarak verebiliriz. Aynı şekilde başka bir örnek ise profesyonel resim işleme programlarından biri olarak tanımlayabileceğimiz Photoshop muadili bulut üzerinden çalışan Adobe Creative Cloud verilebilir.

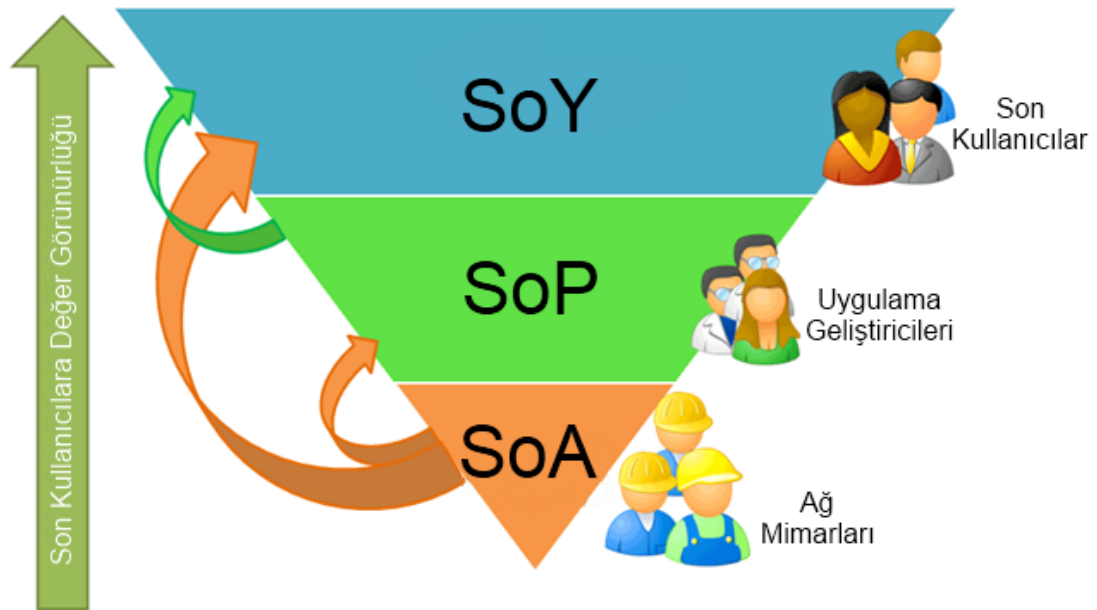
Her geçen gün hizmetlerin buluta kaymasındaki en önemli faktör ise üretilen her bit değerinin gittikçe azalmasına bağlıdır. Yani, sadece bir program üreterek bunu talep kitlesine tek bir sefer para vererek satılması, bir süre sonra marketin tüketilmesi nedeniyle gelir getirmemektedir. Gelir getirmeyen bir programdan zaman geçtikçe destek çekilmekte ve açıklıklar katılmadığından dolayı da program kullanmak tehlikeli olacağından program kullanılmamakta ve ölüme terkedilmektedir. Aynı programın belirli zaman aralığında yeni özellikler eklenerek yeni bir sürümünün çıkarılması ve bunun satılması ise her zaman bir önceki program kadar verimli olmamakla beraber, kullanıcılar tarafından hemen hemen aynı işlev yapan bir programın defalarca satın alınmasına neden olmaktadır. Tahmin edileceği gibi kullanıcılar veya kuruluşlar ihtiyaçlarını gören bir programı sürekli para harcayarak yenilemek istemezler. Bu yüzden genelde her yeni sürüm bir önceki kadar başarılı olmaz. Ayrıca yazılan programların korsanlar tarafından kırılması ile bedava dağıtılması lisans maliyeti zararı dışında, eğer program arka tarafında bir sunucuya bağlı çalışıyorsa ve korsanlar bu programa hiç para vermedikleri halde sunucuya yük bindirerek program geliştiricilerine ilave masraf yaratmaktadırlar.

Görüldüğü gibi günümüzün uygulama piyasası sürdürülebilir bir market değildir. Bunu gören uygulama firmaları artık program satmaktan ziyade, programın sağladığı hizmeti herkes tarafından kullanılacak bir ara yüzden hizmet vermeye doğru yönelmektedirler. Bunu kullanıcılara aylık veya yıllık belli bir ücret karşılığı sunmaktadırlar. Bu şekilde daha fazla kullanıcıya ulaşmakla beraber, kullanıcılardan hizmete göre ücret aldıklarından dolayı sürdürebilir bir ekonomi yaratmış olurlar. Tabi ki bu hizmeti sağlamakta kullanılan yöntem ise bulut bilişim olmaktadır.

2.1.2. BULUT BİLİŞİM SERVİS MODELLERİ

Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü'nün yayınladığı rapora [1] göre bulut bilişim kavramı üç servis modeli ile açıklanmaktadır. Bunlar:

1. **Servis Olarak Yazılım (Software as a Service) (SoY)**, bulut altyapısı üstünde uygulamaların sunulmasıdır. Bu serviste kullanıcılar İnternete bağlandıkları herhangi bir yerden, kendi sistemlerine bir şey yükleme gereği duymadan bulut bilişim üzerinden sunulan uygulamalara erişerek çalışma yapabilirler. Müşteriler uygulamanın kullandığı ağ, depolama alanı, işletim sistemi vb. gibi altyapıları denetlemez ve yönetemezler. Bu tip servislere web tabanlı e-posta servisleri, müşteri ilişkileri yönetimi ve web tabanlı ofis yazılımları vb. dahil edilebilir. Günümüzde bu hizmetlere örnek olarak Salesforce CRM (müşteri ilişkileri yönetimi), Google Apps (rehber, takvim, doküman işleme vb.), Wordpress.com (ağ güncesi hizmeti) verilebilir.



Şekil 2.3 - Bulut Hizmet Modelleri ve Kullanıcıları [2]

2. **Servis Olarak Platform (Platform as a Service) (SoP)**, hizmetinde kullanıcı servis sağlayıcıdan üzerinde kendi uygulamasını geliştirebileceği ve çalıştırabileceği bir platform satın alır veya kiralar. PaaS ortamları geliştirme

araçlarının sunucuda tutulduğu ve geliştirilen uygulamaların çalışacağı ortamlar birlikte gereken tamamlayıcı servisleri de kapsamaktadır. Bu hizmette kullanıcı kurduğu uygulama dışında, platformun altyapısı oluşturan herhangi bir kaynak üzerinde yönetim imkânı yoktur. Bu servislere örnek, Python ve Java programlama dillerine uygulama geliştirilmesine izin veren Google AppEngine, Java/Eclipse tabanlı LongJump ve EC2 üstünde barındırılan ve Java tabanlı görsel geliştirme stüdyosu Wavemaker ve Microsoft Azure Servisleri örnek verilebilir.

3. **Servis Olarak Altyapı (Infrastructure as a Service) (SoA)**, müşterilere altyapının bir servis olarak sunulması modelidir. Bu hizmet genelde sunucu çiftlikleri üzerinde sanallaştırma yapılarak sağlanır. Bulut bilişim için fiziksel donanım temini şekilde özetlenebilir. Kısacası bu hizmette, müşteriler talep ettikleri ve kendinin yapılandırabildiği işlemci, depolama, ağ bant genişliği vb. gibi temel bilişim kaynaklarının üzerine ihtiyacı olan işletim sistemini ve uygulamaları kurabilmektedir. Bu modelin en bilinen örneği Amazon'un sunduğu EC2 (Elastic Compute Cloud) hizmetidir.

Aslında gerçekte üçten fazla bulut bilişim modeli bulunmaktadır. Bu modeller genelde tam olarak bir kategoriye oturmamaktadır. Bazı örnekler:

- **Servis olarak Depolama Alanı (Network as a Service) (SoDA)**, modelinde bulut sağlayıcı kendi altyapısındaki depolama alanını başka bir kuruluş veya kişiye kiralar.
- **Servis olarak Masaüstü (Desktop as a Service) (SoM)**, aslında masaüstü sanallaştırmasıdır. Sanallaştırma ve uygulama aktarımı üzerine dayanmaktadır. Tüm programlar, işlemler ve bilgiler bu sanal masaüstünde çalıştığından dolayı tüm veriler ana bir merkez üzerinde durur.
- **Servis olarak Ağ (Network as a Service) (SoaA)**, telekomünikasyon operatörleri tarafından sağlanan ağ bağlantısı olarak kabul edilebilir.
- **Servis olarak Veri (Data as a Service (SoV)**, modeli tüketici ve sağlayıcının coğrafi konumuna veya örgütsel ayırımına bakılmaksızın, talep halinde verinin sağlanması olarak tanımlanır. Burada veriyi saklayan veya tüketen verinin nasıl saklandığı ile ilgilenmez. Üst seviye bir depolama alanı şeklinde görülebilir. Servis odaklı mimarinin yayılması ile verinin nerde tutulduğu önemini kaybetmiştir.

2.1.3. BULUT BİLİŞİM KURULUM MODELLERİ

2.1.3.1. GENEL BULUT

Genel bulut kısacası bütün verilerin internet üzerinde herkesin erişebileceği bir sunucu üzerinde saklanmasıdır. Veri saklama, hesaplama vb. gibi tüm işlemler üçüncü parti bir şirketin kurduğu altyapı üzerinde kiralanan kaynaklar ile yapılır. Genelde bireylerin kullandığı bir modeldir. E-posta servislerinden Gmail buna örnek verebiliriz. Birden fazla kişinin veya kuruluşun verileri genel bulut sisteminde aynı yapı içinde durmaktadır.

2.1.3.2. ÖZEL BULUT

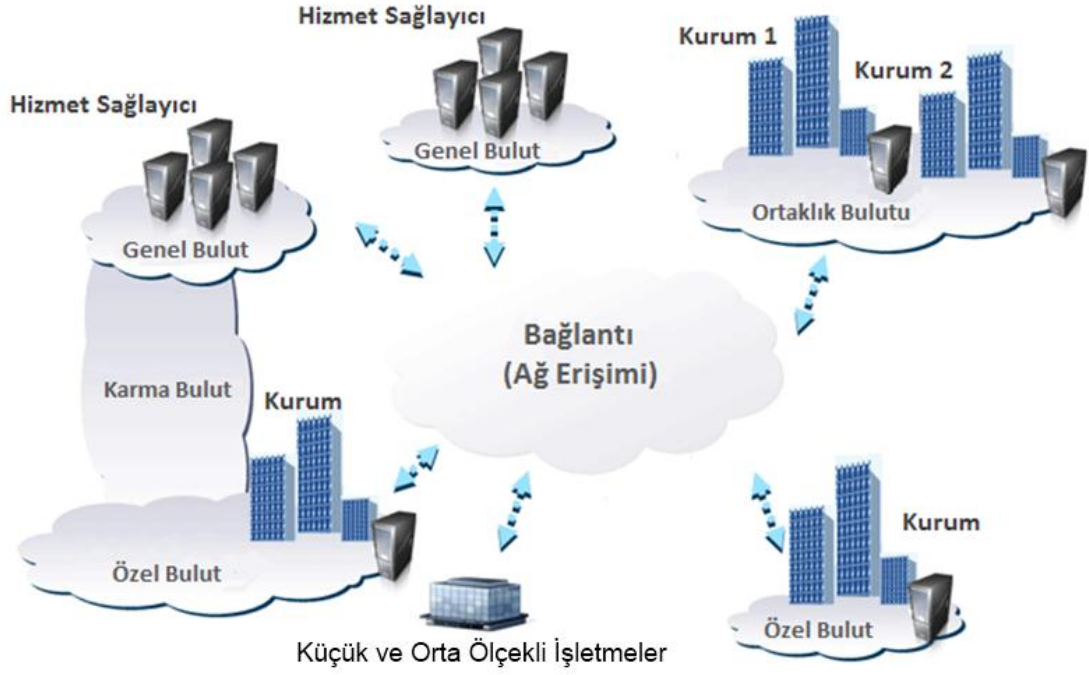
Bir kuruluş kendi içinde kullanmak için kendi bulutunu kuruyor ise, bu kurulum modeline özel bulut denir. Özel bulutun kurulum amacı büyük şirketler için belli bir süre sonra bulut bilişimi kullanmalarının kendi sistemlerini kurmaktan masraflı hala gelmesi ve veri güvenliğini önemseyen ve bu yüzden başkaları ile aynı altyapı kullanarak kendi verilerini riske atmak istememesidir. Kuruluşlar bunu isterlerse kendileri kurabilmelerinin yanında isterlerse üçüncü parti bir şirketten bulut sistemlerini kuruluşa ait fiziksel bir konuma kurarak gerçekleştirebilir.

2.1.3.3. ORTAKLIK BULUTU

Aynı ihtiyaçlara sahip ve altyapısını paylaşmayı kabul eden kurumların bulut bilişim faydalarını fark etmeleri sonucu kurdukları yapıdır. Özel bulutun birden fazla kurum tarafından kullanılan tipi denebilir. Özel buluttan farkı ise, iki farklı kurumun farklı zamanlarda aynı kaynakları kullanması maliyetleri azaltmaktadır.

2.1.3.4. MELEZ BULUT

Şirketlerin güvenlik ve verecekleri hizmetler nedeniyle genel ve özel bulutun birlikte kullanılması sonucu ortaya çıkan yapıdır. Gizliliği fazla önemli olmayan verilerin veya uygulamalar genel bulutu, gizliliği önem taşıyan verilerin ve uygulamalar ise özel bulutu kullanırlar. Örneğin bir firma ürünlerini geliştirmek için özel bulut kullanırken, bu servisleri genel bulut üzerinden sunabilir. Başka bir örnek ise şirket için e-posta servisi için genel bulutun kullanılması, fakat araştırma ve geliştirme için özel bulut kullanılmasıdır.



Şekil 2.4 - Bulut Bilişim Kurulum Modelleri [3]

2.1.4. BULUT BİLİŞİMİN AVANTAJLARI

Bulut bilişim sağladığı avantajlardan biraz bahsetmek gerekirse:

- Düşük Maliyet
- Yüksek Erişilebilirlik
- Platform Bağımsız
- Hizmetin ölçeğini arttırıp azaltabilen - kullandığın kadar öde
- İnternet olan her yerden erişime açık
- Bakım ve yedekleme işlemlerine ihtiyaç duymayan
- Yama ve güvenlik yönetimine ihtiyaç duymayan
- Kolay kaynak kullanımı izleme ve raporlama sunar

2.1.5. BULUT BİLİŞİMİN DEZAVANTAJLARI

Temel anlamda fırsatın olduğu bir yerde risk de bulunmaktadır (Fırsat=Risk). Bulut bilişimde risklerin önemi ve derecesi kurumların [3]:

- Faaliyet alanına,
- İçyapılarına ve ilişkide olduklarına,
- Hizmet sağlayıcı ile kurduğu güven ilişkisine,
- Özel şartlarına göre değişir.

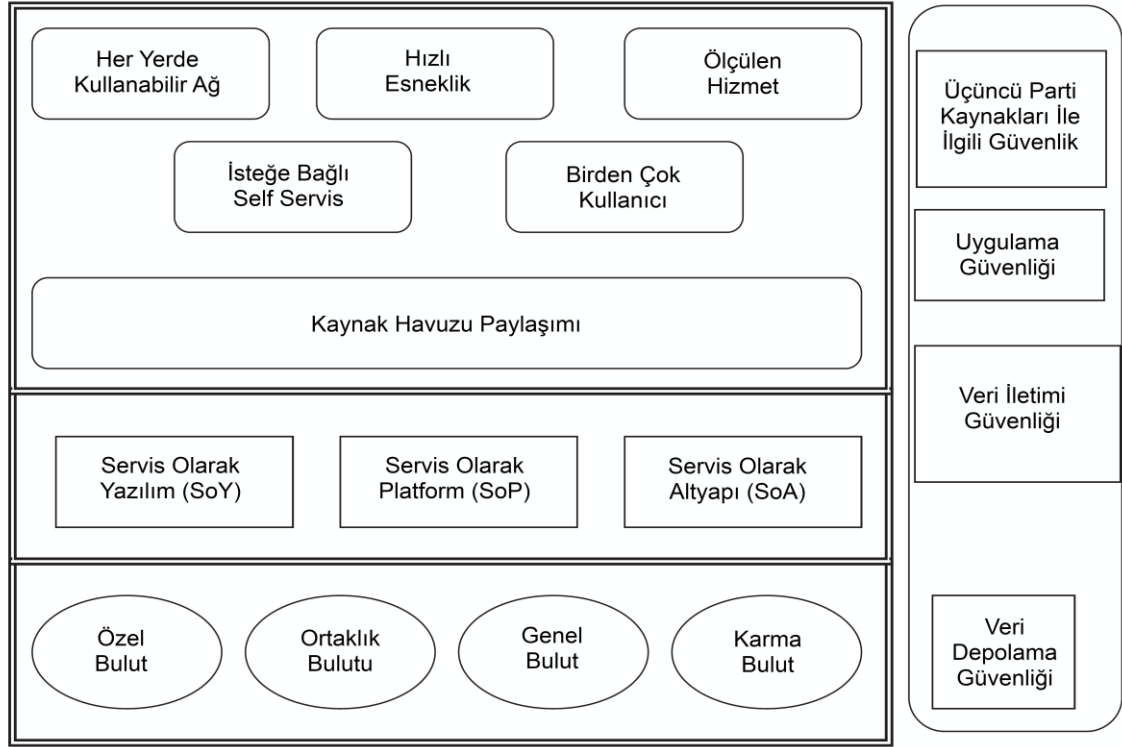
Bulut bilişim riskleri ise aşağıdaki gibi özetlenebilir [3]:

- Hizmet devamlılığı ve kullanılabilirliği
- Veri güvenliği ve gizliliği
- Veri denetlenebilirliği, uyumluluğu ve yasal düzenlemeler
- Hizmet sağlayıcı bağımlılığı ve veri kilitlenmesi
- Yönetim ara yüzü ve uzaktan erişim
- Bant genişliği ve veri transferi
- Yazılım lisanslama

2.1.6. BULUT BİLİŞİMİN GÜVENLİK ANALİZİ

Bulut bilişimin kullanım kolaylığı ve maliyet gibi iki büyük yararı olmakla birlikte, kritik uygulamaların ve hassas verileri halka açık (public) ve paylaşılan ortamlara taşımakla birlikte ortaya önemli güvenlik sorunları çıkmaktadır. Bu sorunlar genelde bütün yapılar için ortak olsa da, en önemli güvenlik sorunları genel bulut yapısında yaşanmaktadır.

Bu sorunların en başını çeken ise veri güvenliğidir. Bulut bilişimde hesaplamalar uzakta yapılabilen fakat günümüzde bulut bilişim daha çok verilerin güvenli bir ortamda saklanması ve rahatlıkla erişebilmesi için kullanılmaktadır. Bu nedenle güvenlik sorunlarının çoğu bulut içerisinde bulunan verinin kim tarafından görüldüğü, olabilecek doğal afetler veya hırsızlıklara karşı korunması ile beraber bir arıza sonucu verilerin nasıl geri getirilmesi ile alakalıdır.



Şekil 2.5 - Bulut Bilişim Güvenlik Karmaşıklığı

2.1.6.1. VERİ GÜVENLİLİĞİ VE GİZLİLİĞİ

Bulut bilişimde veriler ortak ve paylaşılan bir ortamda saklanmaktadır. Genel bulut yapısı düşünüldüğünde hizmet alan kuruluşların birbirlerinin verilerini göremiyor ve değiştiremiyor olması gerekir. Aynı şekilde, şirkete özel bir bulut mimarisinde bir bölümün öbür bölümün verilerini görememesi ve değiştirememesi gerekebilir. Bu noktada veri yalıtımının başarılı bir şekilde yapılması gerekmektedir. Güvenliğin sağlanabilmesi için birçok yöntem bulunmaktadır. Örnek olarak erişim yönetimi ve kullanıcı veya hizmet veren tarafında (hatta iki tarafta) verilerin şifrelenmesi verilebilir.

Veri güvenliği konusunda önemli bir noktada veri transferlerinin güvenli yapılmasıdır. Kullanıcı tarafından gönderilen verilerin veya hizmet sağlayıcı tarafından sunulan verilerin güvenli bir transfer kanalı ile gönderilmesi gerekir. Ayrıca yüksek erişilebilirlik sağlamak amacıyla, hizmet sağlayıcı verilerin dünya üzerinde başka bir noktaya aktarılması sırasında yine bu verilerin güvenliği ve sızdırılmamasına dikkat edilmeli ve güvenli yollar ile yapılması gerekmektedir.

2.1.6.2. ERİŞİLEBİLİRLİK

Tüm verilerin bulutun içinde saklanması, hizmette oluşabilecek bir kesinti anında kurumun servislerinde bir kesintiye neden olacaktır. Bu iki türlü olabilmektedir: hizmet aldığınız sağlayıcınızda oluşabilecek bir kesinti veya kurumunuzun Internet bağlantısında oluşabilecek bir kesinti.

Bulut bilişim, aslında bir kurumun kendi başına oluşturabileceği altyapıdan daha sağlam bir altyapıya sahiptir. Çünkü bir kurumun yedekli hatlarla, yedekli sunucular, yedekli jeneratör, felaket anı için benzer bir veri merkezi ile ulaşabileceği çalışma süresine (uptime), var olan bulut bilişim veri merkezleri ile daha uygun maliyete zaten ulaşabilmektesiniz. Bir kurumun tek başına böyle bir altyapı kurması ciddi bir maliyet gerektirir.

Bir başka yönden bakarsak, kurumumuzda bulunan Internet altyapısında olabilecek bir kesintide aynı şekilde servisleri kesintiye yaratabilir. Bu nedenle kurumda bulunan Internet altyapısının yedekli olması ve gerekli durumlarda farklı ve birbirinden bağımsız tipte hizmetlerden (GDSL ve 3G gibi) yararlanılması gereklidir.

Değnilmesi gereken bir başka konu ise var olan kurum Internet hattının bant genişliğinin bulut bilişimi kaldırabilecek seviyede olması gerekmektedir. Böyle bir bant genişliğine sahip olunmadığı takdirde servis kalitesi düşmektedir.

2.1.6.3. HİZMET BAĞIMLILIĞI

Bulut bilişim kullanırken alınan risklerden en büyüğü verilerinizi başka bir firmanın sunucularında saklamanızdır. Bu noktada verileriniz sakladığınız firmanın iflas etmemesi gerekmektedir. Bunun nedeni ise firmanın yok olması durumunda verilerinize ne olacağının bilmeniz gerekmesidir. Bu sebeple bulut bilişime geçiş yapacak iseniz küresel bir hizmet sağlayıcı ile çalışarak riski azaltabilirsiniz.

Bu hususta dikkat edilmesi gereken başka bir nokta ise, kullandığınız servis sağlayıcının ortak standartlara uymasıdır. İleri ki bir tarihte hizmet sağlayıcınızı değiştirmeniz gerektiğinde, başka bir hizmet sağlayıcınıza bu verileri bir sorun olmadan aktarabilmeniz için bu gereklidir.

Bütün verilerinizi bir firmaya gönderir iseniz, kurumunuzun geleceğini bu firmaya bağlamış olursunuz. Bunun önüne geçmek için, birden çok firma ile

çalışabilirsiniz. Bu şekilde bir firmada yedeğiniz bulunmakta olduğundan riski azaltmış olursunuz.

2.1.6.4. KİMLİK ERİŞİMİ VE YÖNETİMİ

Verilerin koruması gibi doğru kişilerin bu verilere ulaşmasını sağlamakta önemlidir. Kişilerin yetkileri dâhilinde izin verilen verileri görmesi gereklidir. Buradaki risk aslında geleneksel bilgi teknolojinde mevcut olan kimlik erişim yöntemleridir. Kurumda tutulan ve kimin nereye erişebileceğini gösteren erişim kontrol listelerinin bulut yapısıyla uyumlu olması gerekmektedir. Bu iki yolla yapılmaktadır: mevcut bulunan erişim yönetim sisteminin bulut bilişimle bütünleştirilmesi veya bulut bilişim hizmet sağlayıcısının bu altyapıyı size sunması.

Bulut bilişimde hâlihazırda kullanılan iki adet kimlik erişim yönetim protokolü bulunmaktadır: [4]

- **Güvenlik İddialı İşaretleme Dili (GİİD) (Security Assertion Markup Language)(SAML):** Güvenlik İddialı İşaretleme Dili Genişletilebilir İşaretleme Dili (XML) standartları üzerine kurulmuş, yetkilendirme ve kimlik doğrulama özniteliklerini bulut bilişim hizmet sağlayıcısı ile kimlik sağlayıcı arasında takas etmekte kullanılan bir araçtır. GİİD'nin temel hedefi interneti kullanarak tek oturum girişini desteklemektir. Kullanım şeklinin basitçe anlatılması gerekirse, kullanıcının bir kaynağa erişmesi gerektiğinde, hizmet sağlayıcı kullanıcıyı kimlik sağlayıcıya yönlendirir. Sonra kullanıcı kendini kimlik sağlayıcıya tanıtır ve şifrelenmiş GİİD cevabını alır. Bunu hizmet sağlayıcıya gönderir ve sisteme giriş yapar.
- **Açık Kimlik Doğrulama Protokolü (Open Authentication (OAuth) Protocol) :** Açık Kimlik Doğrulama Protokolü bir kurumun veya şahısın özel kaynaklarını bir hizmet sağlayıcıdan başka bir hizmet sağlayıcıya kişinin kullanıcı adı ve parolası gibi kimlik bilgilerinin açığa çıkarmadan paylaşmasını sağlar. Temel hedefi güvenli bir uygulama programla ara yüzüne (API) yetkili erişimi sağlamaktır. Kullanıcı tarafından bakıldığında ise, birden çok hizmet sağlayıcı üzerinde çalışan farklı uygulamalara kimlik bilgilerini dağıtmadan kullanabilmesini sağlar.

Bulut bilişimde neredeyse her şey bir hizmet olarak sunulabildiğinden dolayı, “Servis olarak Kimlik Yönetimi”(Identity Management as a Service (IDaaS)) [4] şeklinde bir model üretilebilir. Böylece kimlik yönetimi de başka bir bulut hizmeti sağlayıcı tarafında yönetilebilir.

2.1.6.5. UYGULAMA GÜVENLİĞİ

Uygulama güvenliğinin günümüzde kullanılan web servislerinden farkı fazla bulunmaktadır. Hâlihazırda bulunan SQL enjeksiyonu, çapraz kod çalıştırma (Cross site scripting) ve çapraz istek sahteciliği (Cross site request forging) gibi saldırılar bulut içinde çalışan programlar içinde aynı şekilde kullanılabilir.

Uygulama güvenliği servis olarak yazılım modelinde önemli bir konu olmaktadır. Örneğin, bulut hizmet sağlayıcı üzerinde bulunan belgelerinizin, bulut hizmet sağlayıcısının kullandığı uygulamadaki (pdf okuyucu veya metin düzenleyici gibi) bir açık nedeni ile başka kişiler tarafından görülmesi ciddi bir güvenlik zafiyeti oluşturmaktadır.

Bu gibi saldırıların engellenmesi ve bulut temelli güvenlik modeli oluşturulmasına katkıda bulunmak amacıyla, bulut bilişim kullanıcılarının anti virüs ve güvenlik yazılımları kurmasına gerek bırakmayan bulut-içi (in-the-cloud) tarama hizmeti, servis sağlayıcılar tarafından başlatıldı. Böylece, bulut kullanıcılarının zararlı yazılımlara, araya girme (man-in-the-middle) saldırılarına ve sistemdeki açık kapılara (loophole) karşı korunmasına, bulut içindeki saldırıların engellenmesine çalışılmaktadır. [5]

2.1.6.6. YASAL UYUMLULUK

Kurumun hangi verilerin, nerede ve nasıl saklandığı yasalar çerçevesinde uyumlu olması gerekir. Yasalarla sorun yaşanabilecek bazı hususlar aşağıda verilmiştir:

- Verinin saklandığı yer, hizmetin verildiği ülke dâhilinde olması gerekebilir. Örneğin bankalarda bulunan müşteri bilgilerinin ülke dışında saklanması yasalarla yasaklanmıştır.
- Verilerin hangi şifreleme algoritmaları ile saklanması seçilirken dikkat edilmelidir. Bazı ülkelerde çeşitli şifreleme algoritmalarının kullanımları

yasalar tarafından yasaklanmıştır ve kullanılması durumunda cezalar verilmektedir.

- Bazı tipteki verilerin bulut ortamında saklanması bazı ülkelerde yasalar tarafından sınırlandırılmıştır.
- Bazı tipteki verilerin bazı ülkelere aktarılması veya orada görüntülenmesi yasaklanmıştır.
- Bilgilerinizi fiziksel olarak saklandığı ülkedeki yasalar, gerek görüldüğü takdirde sizin verilerinize el koyulmasına neden olabilir. Buna en güzel örnek Amerika'daki yasaların Amerikan hükumetine ve diğer birimlerine kurumlara ait bilgilere bile erişimin için neredeyse sınırsız haklar tanımakta.
- Hizmet sağlayıcı ile bir sorun oldu mu mahkeme yeri neresi olacak?
- Veri merkezi bir felaket ile karşı karşıya gelirse, bilgilerin güvenliği hangi yasalar ile kimler tarafından korunacak?
- Bulut bilişim altyapısına veya uygulamalarına oluşabilecek bir saldırı hangi ülkenin, hangi yasası, ne şekilde koruyor?

2.1.7. ÖLÇEKLENDİRİLEBİLİR BULUT BİLİŞİM GÜVENLİĞİ

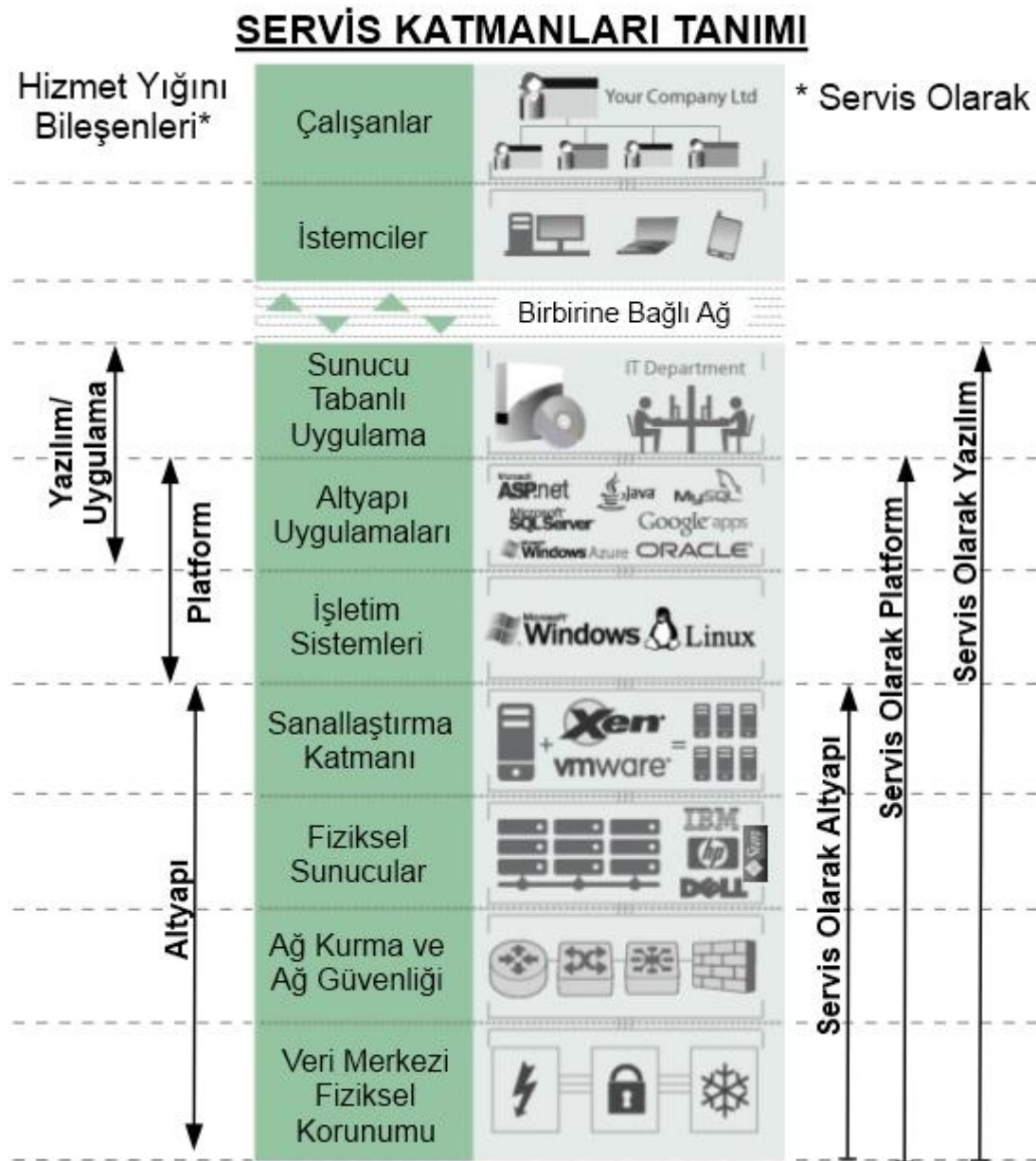
Bulut bilişim sunduğu hizmetlere göre farklı hizmet modellerine ayrılmaktadır. Farklı hizmet modellerinin farklı güvenlik gerektirmektedir. Bu durum güvenlik anlayışında verilen hizmete göre farklı güvenlik önlemlerinin alınmasına neden olmaktadır.

Tablo 2.1 - Bulut Bilişim Güvenlik Gereksinimleri

Bilgi Güvenliği Gereksinimleri	Bulut Kurulum Modelleri					
	Genel			Özel		
	Bulut Servis Modelleri					
	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS
Mevcut Olma	X	X	*	X	X	X
Yetkilendirme	X	X	X	*	*	X
Gizlilik	*	*	X	*	X	X
Bütünlük	X	*	X	*	X	X
Kimlik Doğrulama	X	*	X	X	*	X

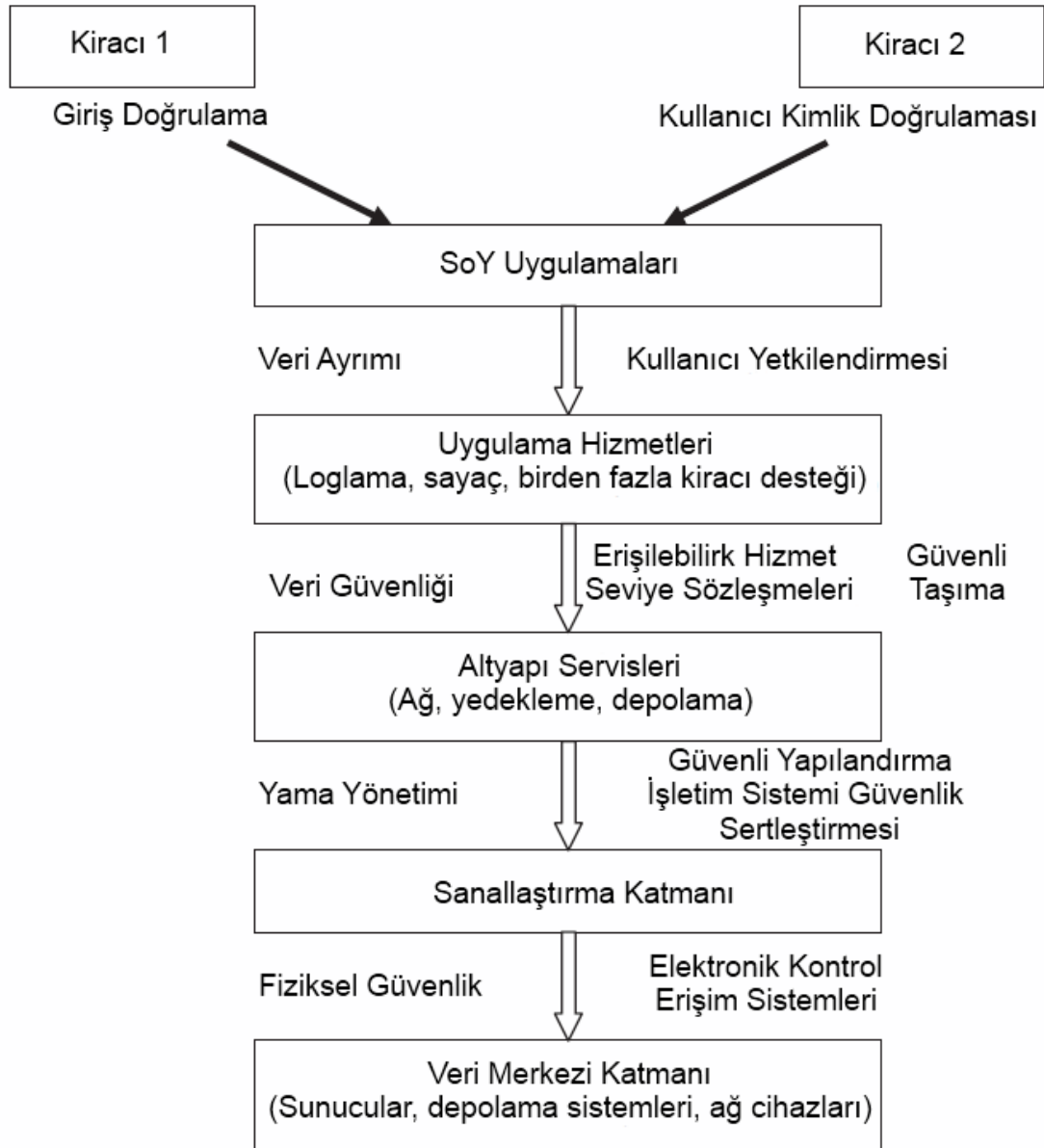
X Gerekli ihtiyaçlar * Opsiyonel ihtiyaçlar

Tablo 2.1’de NIST tarafından bulut bilişim tanımında kullanılan bulut servis modellerindeki güvenlik ihtiyaçları verilmiştir. Temel olarak ölçeklendirilebilir güvenlik, hizmet modelleri olan SoA, SoP ve SoY arasındaki farklılıktan oluşmaktadır. SoA modelinde altyapı güvenliği bulut sağlayıcıya düşmekte iken, SoY’da ise verilen servisteki tüm güvenlik önlemleri bulut sağlayıcıya düşmektedir. SoA modelinde altyapı güvenliği dışında kalan, yazılım ve işletim sistemi güvenliği ise kullanıcıya düşmektedir. Fakat bulut sağlayıcılar bütün hizmetleri aynı altyapı ile verdiklerinden dolayı, çoğu gereksiz güvenlik önlemleri ve politikaları uygulanmakta ve bu gereksiz masraflara ve sistem yavaşlamasına neden olmaktadır.



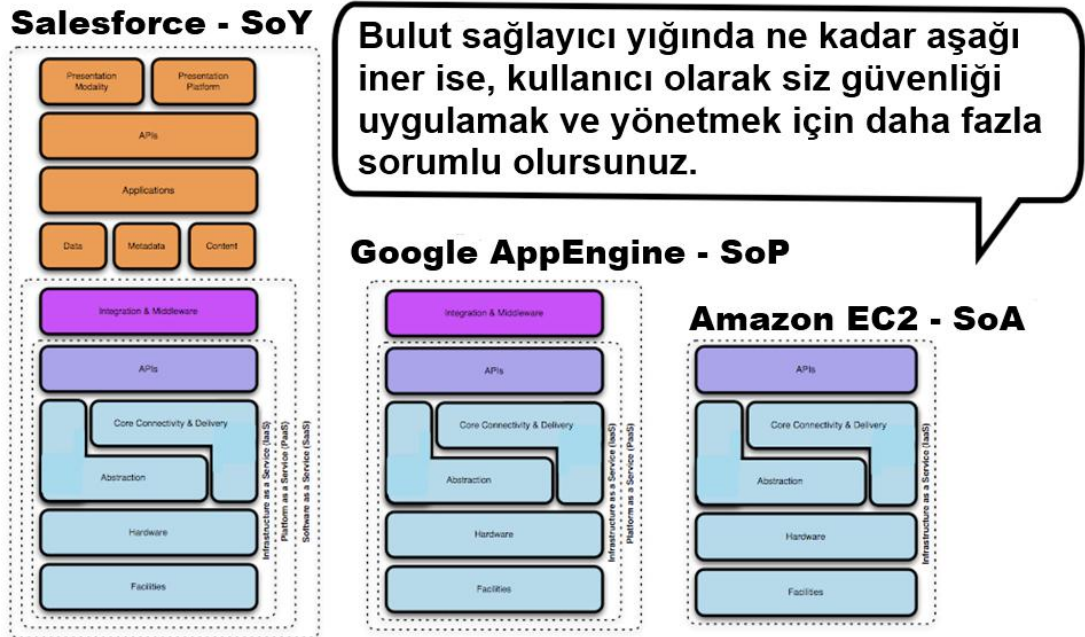
Şekil 2.6 – Farklı Servis Modellerinin Sorumlu Olduğu Kısımlar [6]

Şekil 2.6’da görüldüğü üzere, verilen servisin şekline göre bulut sağlayıcının sorumlu olduğu katmanlar değişmektedir. SoA sisteminde bağlayıcı sanallaştırma katmanına kadar sorumluluk sahibi iken, SoP yapısında işletim sistemi ve altyapı yazılımları ile de sorumlu olmakta iken, SoY hizmeti verdiği grupta ise sistem üzerinde kurulmuş yazılımın güvenliğinden de sorumlu olmakta. Bu şemada yukarı doğru gidildiğinde bulut bilişim sağlayıcının sorumluluğu artmakta ve kullanıcının sorumluluğu düşmekte ve işi kolaylaşmaktadır.



Şekil 2.7 - Servis olarak Yazılım Güvenlik Yığını

Tipik bir SoY hizmetinde güvenlik Şekil 2.7'deki gibi birden fazla kiracının yapacağı farklı işlemler bulunur. Bunlar ilk önce SoY hizmetindeki uygulamalar tarafından değerlendirilir. Bu katmandan bir alta bulunan uygulama katmanlarına geçerken veri ayırım sorunu ve kullanıcı yetkilendirmesi sonucunda çıkacak güvenlik sorunlarına dikkat edilmektedir. Bir alta ki altyapı katmanına geçerken ise veri güvenliği ve bulut sağlayıcı ile yapılan güvenli transferi bulunması ile alakalı hizmet seviye sözleşmesi güvenlik sorunlarına bakılmalıdır. Bunun altında yer alan ve bulut bilişimin temelini oluşturan sanallaştırma katmanında ise yama yönetimi ve işletim sisteminin güvenli olması için yapılan sertleştirilme yapılandırması gibi durumlar bulunmaktadır. En son olan ve fiziksel olan veri merkezi katmanında ise fiziksel güvenlikle beraber elektronik erişim kontrol sistemlerinin güvenliği yer almaktadır. Burada görülen sistemlerin hepsi SaaS katmanında bulut bilişim sağlayıcıya düşmekte ve büyük bir yatırım gerektirmektedir.



Şekil 2.8 - Bazı Örnek Bulut Hizmetlerinde Sorumlu Olunan Kısımlar [7]

2.2. OYUN TEORİSİ

2.2.1. OYUN TEORİSİ NEDİR?

Oyun teorisi, birden fazla karar vericinin birbiri ile etkileşime girdiğinde ki olayı gözlemlemek amacıyla tasarlanmış analitik araçlar topluluğudur.

Oyun teorisi karar vericilerin davranışlarını değiştirmek istemediği denge anını bulmaya çalışır. Yapılan seçimler bir karakteristik fonksiyona konarak iki veya daha fazla tarafından yapılan seçimlerden ne kazanacağı ve kaybedeceği belirlenir. Kazanımlar ve kayıplar çözüm matrisi adı verilen matris altına toplanılır. Bu şekilde hangi oyuncunun neyi, ne durumda iken, nasıl seçeceği ortaya atılır.

Oyun teorisi modellemesinin amacı insanların neden belirli bir şekilde davrandığı ve yaptıkları bu davranışlara göre gelecekte ne gibi davranışlar sergileyeceklerini açıklamaktır. Bu teorinin arkasında bulunan basit varsayımlar; oyuncular başkaları hakkında inanç oluştururlar, bu varsayımlara göre en iyi cevabı verirler ve oyuncular arasında ortak bir bilgidir. Dolayısıyla, bir oyunda her oyuncu karşısındakinin uygulayacağı stratejiye göre kendi için ideal stratejiyi seçer.

Tablo 2.2 - Tutsak İkilemi Çözüm Matrisi

		ZANLI 2	
ZANLI 1		İtiraf	İnkâr
	İtiraf	2,2	7,0
	İnkâr	0,7	5,5

Oyun teorisi, her bir oyuncu için oyunun kıstaslarına göre bir karakteristik fonksiyon oluşturarak, farklı seçeneklerde her bir oyuncunun ne kadar bedel ödediğine veya kazandığını gösterir. Bu bedeller hesaplandıktan sonra bir oyuncunun seçtiği eylem, diğer oyuncuların seçtikleri eylemlere bakıldığında oynanabilecek en iyi seçenek ise, bu eylemin o oyuncu tarafından seçildiği var sayılır. Eğer bu tüm oyuncular için geçerli ise, kısacası, hiçbir oyuncu, rakip oyuncunun stratejisi sabit

kaldığı sürece kendi eylemini değiştirerek kazanç sağlayamamakta ise, bu oyunun dengede olduğunu belirtir ve bu dengeye Nash dengesi denmektedir.

Oyun teorisinin kullanımına bir örnek vermek için tablo 2.2’de gösterilen ve oyun teorisinin en çok bilinen oyunlardan biri olan tutsak ikilemini inceleyelim. Tutsak ikilemi özellikle sosyal bilimlerde en çok tanınan strateji oyunlarından biridir. Oyunu biraz açıklamak gerekirse, iki kişi polis tarafından zan altına alınmıştır. Fakat polisin elinde yeterli kanıt olmadığı için kimin suçlu olduğu bilinmemektedir. İki zanlı farklı sorgu odalarına alınır. Zanlılara bir anlaşma sunulur. Eğer zanlılardan biri diğerinin aleyhinde tanıklık yapar ve diğer zanlı suskun kalır ise, suskun kalan 7 sene hapis cezası, aleyhinde tanıklık yapan ise hapis cezası almayacaktır. Eğer iki zanlıda birbirini aleyhinde tanıklık yapar ise, her iki zanlı 5’er yıl hapis cezası alacaktır. Eğer her ikisi de suskun kalmayı tercih ederlerse, bu sefer her zanlı 2’şer sene ceza görecektir.

Verilen koşullar altında her iki zanlı iki seçenektan birini oynamak zorunda bırakılmıştır. İki zanlı farklı odalarda bulunduğundan dolayı birbirlerinin kararlarını kendi kararlarını verene kadar öğrenemeyeceklerdir. Oyun incelendiğinde görülecektir ki diğer zanlının seçeneğine bakılmaksızın, her zanlı diğer zanlının aleyhinde tanıklık yapar ise kaybı en aza inecektir. Yani, eğer iki numaralı zanlı suskun kalır ise, bir numaralı zanlı iki numaralı zanlının aleyhinde tanıklık yapması suskun kalmasından daha az kayba neden olmaktadır. Kısacası, suskun kalır ise 2 sene ceza alacağına, aleyhinde tanıklık yapıp serbest kalmayı tercih eder. Eğer iki numaralı zanlı bir numaralı zanlının aleyhinde tanıklık yapar ise, bir numaralı zanlı suskun kalması kendisine 7 sene hapis cezasına mal olmakta iken, iki numaralı zanlı hakkında aleyhinde tanıklık yapması 5 sene hapis cezasına neden olmaktadır. Aynı koşullar ikinci zanlı içinde geçerlidir.

Yapılabilecek hareketler incelendiğinde ortaya çıkan sonuç gösteriyor ki iki tarafında yapacağı rasyonel seçim aleyhinde tanıklık yapmak olmaktadır. Bu şekilde iki zanlıda beşer sene hapis yatacaktır. Fakat çözüm matrisi dikkatli incelenir ise eğer iki zanlının da suskun kalması sonucu alacakları hapis cezasının iki sene olduğu görünebilir. Birbirleri ile etkileşime giremeyen iki oyuncunun rasyonel davranarak aldıkları karar az yatabilecekleri hapis cezasını artmasına neden olmuştur.

2.2.2. OYUN TEORİSİ GÜVENLİK MODELLEMESİ

Oyun teorisi güvenlik modellemesinde, saldırı ve savunma güvenlik mekanizmaları arasındaki ilişki incelenmektedir. Güvenlik konusunda ise oyun teorisi, savunanın ve saldırganın belirli olasılıklarla seçeceği stratejilere göre, ideal savunma veya saldırı stratejisi seçilmesinde yardım etmektedir. Bu saldırgan ve savunan (bulut sağlayıcı veya sistem yöneticisi) arasında oynan bir oyundur. Oyun sıra ile oynanmaktadır. Yani savunan mekanizmasını geliştirdikten sonra saldırgan saldırı yapmaktadır. Daha sonra yapılan saldırıya göre savunan savunma mekanizmasında değişiklik yapmaktadır (veya yapmamakta). Daha sonra tekrar saldırgan saldırmayı dener ve oyun bu şekilde devam etmektedir. Görüldüğü gibi oyun tekrarlanan bir oyun olmakta ve bir kere savunma veya saldırma ile bitmemektedir.

Burada oynanan oyundaki en önemli özellik ise iki tarafın birbirlerinden bilgi saklamasıdır. Bu tipte oyunlara oyun teorisinde bayesian oyunu (game with incomplete information) denmektedir. Bu oyun modellenirken oyuna yeni bir oyuncu olarak doğa (nature) eklenir. Doğa oyuncuların yapacakları eylemlere farklı olasılıklar vererek oyunu şekillendirir. Bu verilen olasılıklar oyunda bulunan oyuncuların kazançlarını etkilemektedir. Oyunun bayesian olarak adlandırılması burada verilen olasılıklardan kaynaklanmaktadır. Oyuncuların diğer oyuncular hakkında farklı inançları olmakta ve buna göre hareket etmektedirler.

Oyun teorisinin güvenlik alanında kullanılmasına tablo 2.3’de bulunan oyun örnek verilebilir. Polis kuvvetlerinin iki adet terminali olan bir havaalanını koruduklarını ve bir terörist grubunun da bu terminallere saldırı düzenlemek istedikleri bu oyunda varsayılır. Bu oyundaki sorun polis kuvvetlerinin aynı anda sadece bir tane terminali koruyabilmektedirler. Tablo 2.3’de görüldüğü gibi terminal-1 önemi terminal ikiye göre yüksektir. Başka bir deyişle hedeflerin farklı ağırlıkları bulunmaktadır.

Polis kuvvetlerinin bu oyunda birinci terminalin daha değerli olduğunu görüp sadece birinci terminali korumaya çalışır. Saldırgan polisin birinci terminali koruduğunu gözlemler ve ikinci terminale saldırır. Bu durumda polis negatif saldırgan ise negatif bir sonuç alır. Polis bu durumda taktik değiştirip sadece ikinci

terminali korur ise, saldırgan bunu gözlemleyip bu seferde birinci terminale saldırı düzenler. Yine aynı şekilde polis negatif, teröristler ise pozitif sonuç alırlar. Burada ki sorun deterministlik bir savunma yöntemi gözlemlenebilir olduğundan saldırgan bu sistemi gözleyebilip yararlanabilmektedir.

Tablo 2.3 - Polis ve Saldırgan Arasında Geçen Güvenlik Oyunu



	Terminal - 1	Terminal - 2
Terminal - 1	5, -3	-1, 1
Terminal - 2	-5, 5	2, -1

Polisin dinamik ve rastgele bir güvenlik yapısı izlemesi saldırgan tarafından yapılan gözlemlemeyi geçersiz kılmaktadır. Örneğin polis günün %60'ında birinci terminali, günün %40'ında ikinci terminali korur ise ve her gün terminalleri koruduğu saatleri veya koruma oranlarını değiştirir ise, saldırgan yaptığı gözlemler bir sonraki gün şartlar değiştiğinden dolayı hiçbir işe yaramayacaktır. Bu durum saldırganların kararsızlığını ve maliyetleri yükseltmekte, polisin pozitif bir sonuçla çıkma olasılığını artırmaktadır. Bu tip oyunlara Bayesian Stackelberg Oyunları denmektedir. Stackelberg oyunlarının özelliği, oyunda ilk hareketin güvenlik tarafından yapılmasıdır. Daha sonra saldırgan bu harekete cevap verir. Bayesian özelliği ise saldırgan tipinin belirsiz olmasına bağlıdır.

Bulut bilişimde servis modelleri kişilerin yaptığı seçimlere göre farklılık göstermektedir. Bu seçimlere göre ölçeklendirilebilir güvenlik değerlendirmesi ve risk yöntemi yapılabilir. Bu yöntem bulut bilişim riskleri ve servis modelleri göz önüne alınarak güvenlik önleminin maliyetinin, o önlemin engelleyeceği riskin vereceği zararı ile karşılaştırma yapabilmesini sağlayabilir. Servis modellerine uygun kalıplar (saldırı çeşitleri) belirlenerek bu kalıplar üzerinde bu oyun oynanır. Birden fazla kalıp birden fazla servis modeli içinde yer alabilmesine rağmen, farklı servis modellerinde edinilecek kazanç farklı olacağından, farklı seçimler yapılabilir.

2.2.3. OYUN TEORİSİNİN GÜVENLİK ALANINDA KULLANIMI

Oyun teorisinin fiziksel ve sanal ortamlarda kullanımı her geçen gün artmaktadır. Özellikle dinamik değişme gösteren ortamlarda statik savunma sistemlerinin yetersizliği, oyun teorisine yönelimi neden olmuştur.

Los Angeles havaalanının fiziksel güvenliği için kullanılan oyun teorisi ile çalışan ARMOR (Assistant for Randomized Monitoring Over Routes) (Yolları Rastgele İnceleme Yardımcısı) [8] programı, oyun teorisinin günümüz dünyasında kullanılan örneklerinden bir tanesidir. Güvenlik kuvvetlerinin havaalanının her bölgesinde aynı anda kontrol edebilecek insan ve K-9 devriye kaynakları bulunmamaktadır. Deterministlik bir plan yapılması saldırganların gözlemlemesi sonucu etkisiz halde kalmaktadır. ARMOR bu sorunu önceden kestirilemeyecek şekilde planlama yaparak çözmektedir. Burada bahsedilen rastgelelik zar atılmasındaki gibi gelişigüzel değil, hedefteki varlıkların önemlilik derecesine göre sınıflandırılmış ve akıllı rastgelelik olarak değerlendirilmektedir.

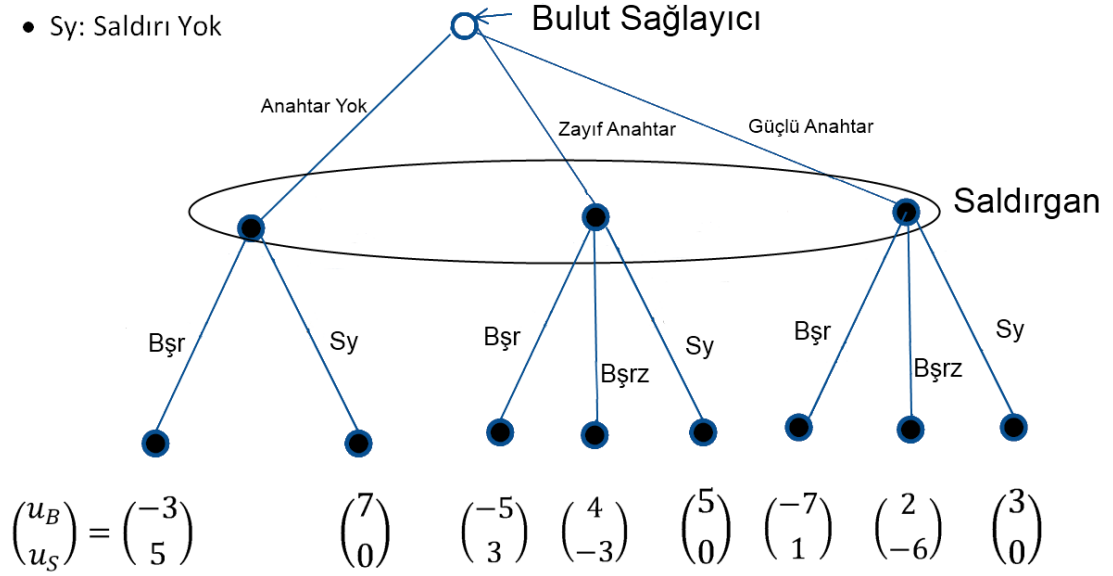
Sanal ortamda yapılan saldırıları modellemek içinde oyun teorisi kullanılabilir. Yakın zamanlardaki [9] [10] [11] [12] çalışmalarında saldırı tespit sistemlerinin ve saldırganların birbirleri ile etkileşimleri oyun teorisi kullanılarak modellendi. Bu modellemede temel olarak kullanılan özellik saldırganın hedef sisteme saldırma amacıdır. Saldırı tespit sistemleri ve saldırgan arasındaki etkileşimin oyun teorisi açısından incelenmesi, ağ saldırılarında saldırganların yapacakları hareketlerin saldırıdan önce veya saldırı anında gerçek zamanlı tahmin edilmesine olanak verdi.

2.2.4. OYUN TEORİSİNİ KULLANAN BİR GÜVENLİK ÖRNEĞİ

Saldırgan yapabileceği farklı saldırı çeşitlerinin farklı hizmet modelleri üstündeki etkisi incelenmesi gerekmektedir.

Örnek olarak Şekil 2.9’da “Veri saklamada veya Transferinde Kullanılacak Şifreleme Anahtarı Uzunluğu (Güçlülüğü)” incelenmiştir.

- Bşr: Başarılı Saldırı
- Bşrz: Başarısız Saldırı
- Sy: Saldırı Yok



Şekil 2.9 - Bir Bulut Oyun Teorisi Güvenlik Örneği

Bu örnekte bir saldırganın bir bulut bilişim sağlayıcısına uyguladığı saldırı modellenmiştir. İlk önce bulut sağlayıcı gelebilecek saldırılara göre önlem almalıdır. Bu önlemler aşağıdaki şekilde olabilir:

- Anahtar Yok (güvenlik yok)
- Zayıf Anahtar (zayıf güvenlik)
- Güçlü Anahtar (güçlü güvenlik)

Her bir seçeneğin karakteristik fonksiyonla hesaplanacak kazanca etkisi bulunmaktadır. Alınacak güvenliğe göre fazla elektrik harcanıp performans kaybı yaşanacak ve güvenliğin uygulanabilmesi için masraflar olacaktır.

Aynı şekilde saldırgan ise alınacak güvenlik önlemine göre bir saldırıda bulunacak ve bu saldırının başarısına karakteristik fonksiyonda kazancı belirlenecektir. Az veya güçlü güvenliği olan bir sisteme saldırabilmesi için normalden daha fazla hesaplama gerektiren işlemler yapacak ve daha fazla zaman harcayacaktır. Bunun sonucunda eline geçen bilgi işe yaramaz bir bilgi ise, hiç saldırı yapmadığı duruma göre saldırgan bir zarara uğramış olacak. Saldırgan bir daha ki saldırısında bunu değerlendirerek, bulut sağlayıcıya saldırmaktan vazgeçecektir.

Bu şekilde oyun sürekli devam etmekte olup, bulut sağlayıcı saldırganların saldırmadığını fark ettiği anda kendi masraflarını azaltmak için güvenlik politikalarını ve önlemlerini hafifletebilir. Saldırganlarda bunu görüp tekrar saldırmaya başlayıp, bulut sağlayıcı yüksek güvenlik önlemlerini tekrar aldirmayı zorlayabilir.

Burada daha öncede bahsettiğimiz gibi, iki tarafında davranışların değiştirmek istemediği bir denge anı bulunması hedeflenmektedir. Bu denge anı farklı hizmet modellerinde farklı şekilde olmaktadır. Örneğin SoY'da bütün bilgiler önemli olabilirken, altyapı olarak kullanılan SoA sistemlerde bulunan dosyalar gerekli olmayabilir. Herkesin erişimine açık olabilir.

2.3. BULUT BİLİŞİM GÜVENLİĞİ İLE İLGİLİ ÇALIŞMALAR

Bulut bilişim piyasada bir süredir bulunmasına rağmen yeni yeni yaygınlaşan bir hizmet modelidir. Bulut bilişimde güvenlik değerlendirmesi de bu bağlamda yeni bir konu olduğundan dolayı, bu konuda yapılan çalışmalar da nispeten yenidir. Yapılan çalışmaların büyük bir kısmı ise sadece ızgara hesaplama modeli düşünülerek yapıldığından dolayı, bulut bilişimin tamamını kapsamamaktadır. Günümüzdeki bilgi teknolojilerinden farklı olması nedeniyle, günümüzdeki sistemlere uygulanan güvenlik ve risk değerlendirme yöntemleri bulut bilişimde ya uygulanamamakta ya da yetersiz kalmaktadır.

Kupsch, Miller, Heymann ve César önerdikleri modelde [13], bulut bilişimden daha çok ızgara hesaplama yapan sistemlerde program ile donanım arasında çalışan katmana uygulanabilmektedir. Temel olarak bulut bilişimle benzer olsa da, bulut bilişimde, özellikle SoA ve SoP hizmetinde, verilen altyapının üzerine kullanıcılar kendi hizmetlerini kurduklarından dolayı, bu yöntem yetersiz kalmaktadır.

Temel olarak bu yöntemde, ilk önce verilen işlerin hangi varlıklarla ilişkiye girdiği ile alakalı bir ağaç çıkarılmaktadır. Sonrasında bu ağaç içindeki her düğümün birbirleri ile ilişkisi incelenmekte ve burada oluşabilecek açıklıklar bulunmaktadır. Daha sonra bu kısımların kodları daha önceden ağaç yönetiminden çıkabilecek açıklıklar göz önüne alınarak uzmanlar tarafından elle incelemektedir.

Bu yöntemin en büyük sorunu bulut bilişimde kullanılan uygulama programı arabirimlerinin çok büyük olması ve özellikle SoA ve SoP hizmetlerinde incelemenin kısıtlı olmasının yanı sıra elle inceleme işleminin çok uzun sürmesidir. Ayrıca ızgara hesaplama ile bulut bilişim teknolojileri bazı kısımlarda aynı görevi görse de, riskleri birbirinden farklıdır.

Peiyu ve Dong bulut bilişim için üç katmanlı risk değerlendirme modeli önermişlerdir [14]:

- **Katman 1:** İlk aşamada problem hiyerarşik bir düzende formülleştirilmektedir. En üst katman ulaşılabilecek amacı belirtmektedir. Bu modelde ilk katman bütün olarak bulut bilişim platformunu karşılık gelmektedir.
- **Katman 2:** Bu katman, birinci katmanın değerlendirilmesi için 8 adet özellik içermektedir.
- **Katman 3:** Karar çerçevesinde somut değerlendirmenin yapıldığı son bölümdür. Üsteki katmanlarla ve özel durumlarla ilgili 39 farklı faktör belirlenmiştir.

AHP (Analytic Hierarchy Process) (Analitik Hiyerarşi Süreci) gerçekleştirilmesi 3 prensibe bağlıdır: Ayırıştırma, birbirleri ile karşılaştırma ve ağırlık sentezi. AHP yönteminin bulut bilişim mimarisi üzerinde bazı avantajları bulunmaktadır. Bunlar:

- Problemi hiyerarşik parçalara bölebilmek,
- Nitelikli veri bulunmayan durumlarda karar vericinin deneyimlerinden faydalına bilmek.

Karar vericiye (uzman) bağlı olarak katman 3'deki faktörlere göre değerlendirme yapılır ve hepsine bir ağırlık verilerek bir matriste toplanıp bir ağırlık vektörü elde edilir.

Burada bulunan sorun karar veren kişilerin yaptığı değerlendirmeler tutarlılık doğrulamasından geçmediği sürece, karar verenlerin formlarını tutarlılıktan geçene kadar elle bu vektörleri değiştirmek zorunda kalmalıdır.

Jordi Guitart J. Oriol Fitó [15] önerdiği yöntemde, yarı-nicel bir karşılaştırma yapılmaktadır. Yapılan karşılaştırmada öncelik kullanıcı memnuniyeti veya elde

edilen karın artırılması gibi iş düzeyi hedefi konularıdır. Bu şekilde yapılan yarı-nicel karşılaştırma, bazı riskleri kazanç olarak görmekte ve ileride çıkarabileceği sorunları göz önüne almamaktadır. Ayrıca bu çalışmada etki(impact) iki faktör arasında değişmektedir: Kazanç ve tehdit. Karşılaştırma yapılmadan önce riskler şu şekilde gruplanmaktadır:

- Riskli bir olayın gözlenme olasılığı: 1-5 arasında değer almakta. 1 değeri 20 yılda bir, 2 değeri yıllık, 3 değeri aylık, 4 değeri günlük ve 5 değeri ise her an olabilirliği belirtmekte,
- Olayın vereceği darbe; bir tehdit, kazanç veya her ikisi: Çok yüksek (-5 veya 5 negatif ve pozitif darbe), yüksek (-4/4), orta (-3/3), düşük (-2/2) ve çok düşük (-1/1).

Bu yöntemde kısaca risk, riskli olayın gözlenme olasılığı ile olayın vereceği darbenin birbiri ile çarpılması sonucu çıkan -25 ve 25 arasında değerler ile ölçülmekte olup, mantıksal olarak dar bir kıstasa sokulmaktadır. Önerdiğimiz yöntemde, hizmet modeline göre sunucunun varlık olarak değerinin 0 ile 100 gibi geniş bir aralıkta verilebilmesinin dışında, oluşan risklerin her zaman sisteme etkisi kötü olacağı düşünülerek, gelecekte olabilecek sorunları şu an kendimize kar olarak dönüştürmek yerine, gelecekteki sorunu bertaraf etmeği önemsemekteyiz.

M. Kiran, Ming Jiang, D.J. Armstrong, and K. Djemame [16] yazdığı makalede belirtildiği gibi, bulut bilişim için önerilen risk değerlendirme yöntemlerinin çoğunluğunun son kullanıcının bakış açısına odaklanmaktadır. Bu makalede ve önerilen yöntemde ise servis sağlayıcısının gözünden bakılmaktadır. Bahsedilen yöntemler bu konuda birbirlerine benzedi, [16] çalışmasında önerilen yönteminde bulut servislerini iki kategoriye ayırmaktadır: Servis sağlayıcılar ve altyapı sağlayıcılar. Servis sağlayıcılar aslında altyapı sağlayıcılardan hizmet satın olarak son kullanıcıya ileten bir kurum olarak ele alınmaktadır. Bu şekilde servis sağlayıcılar ve altyapı sağlayıcılar çeşitli faktörlere (bazı zaman ikisinde de aynı faktörler) farklı ağırlıklar vererek birbirleri arasında risk değerlendirmesini yapmaktadır. Bu değerlendirme risklerin kategoriye ayrılması ile devam eder ve daha sonra bu kategorilere göre risklerin nasıl bertaraf edileceği veya ihmal edilip edilemeyeceği değerlendirilir.

Önerdiğimiz yöntemde, kullanılabilecek her servis tipi bir modele ayrılabilir. Böylece bulut servisleri bir önceki anlatılan makaledeki yöntemle

göre sadece servis sağlayıcı ve altyapı sağlayıcı olarak basit iki parçaya ayrılmaz, verilen hizmete göre istediği kadar modele ayrılabilir. Giriş bölümünde belirtildiği gibi, bulut hizmet modelleri NIST'in tanımladığı SoY, SoA ve SoP üç model dışında, SoaA (Servis olarak ağ), şirket yedeklemesi veya tekil kişilerin kullandığı SoDA (Servis olarak Depolama Alanı) ve işyerlerinin elemanlarının bilgisayarlarını buluta aktaran SoM (Servis Olarak Masaüstü) gibi çeşitli modelleri de kapsamaktadır. Bir önceki makalede [16] servis sağlayıcı olarak SoY görür isek, geri kalan her şey altyapı sağlayıcı olarak değerlendirilmekte bu yüzden örneğin SoDA ve SoA arasındaki farklar ihmal edilmektedir. Önerdiğimiz yöntemde saldırının etkileyebileceği her model, ölçeklendirilebilir bir şekilde birbiri ile karşılaştırılmaktadır.

Genelde risk değerlendirme modelleri uzun zaman sürmekte ve yavaş işlemektedir. Önerdiğimiz model, diğer modellerden farklı olarak oyun teorisine bağlı bir oyun oluşturduğundan ve servis sağlayıcının zarar görebilecek değerlerini kendisinin geçmiş olaylara göre belirlemesi özelliğine sahip olduğundan, diğer modellere göre daha çabuk ve bulut sağlayıcıya özgün bir hesaplama yapılmasını sağlamaktadır.

3. OYUN TEORİSİ KULLANARAK BULUT BİLİŞİM RİSK DEĞERLENDİRME MODELİ

Güvenlik modellemesi yapılırken tehditlerin hesaplanması güvenlik değerlendirmesinin en önemli parçasıdır. Güvenlik açıklığı önde gelen bir risk faktörüdür. Risk, ISO 27005 içinde şu şekilde tanımlanmıştır: “Bir tehdidin, tek bir varlığın veya varlıkların güvenlik açıklarından faydalanarak organizasyona zarar verme potansiyelidir”.

Bulut bilişimdeki temel varlıklar basit olarak ikiye ayrılmaktadır.

- Veriler
- Fonksiyonlar/Uygulamalar/İşlemler

Bu ihtiyaçlara göre aşağıdaki oyun teorisi varsayımlar yapılmıştır.

- Savunan ve saldırgan bu oyunda birer oyuncu olmaktadır. Birden çok saldırgan var ise bunlar işbirliği yaparak saldırının oluşturulduğu, birden çok savunan var ise işbirliği yaparak savunma oluşturulduğu var sayılmaktadır.
- Her saldırganın saldırı kabiliyeti ortak sayılmaktadır. Böylece tipik saldırılarda her saldırganın eşit saldırı olasılığı bulunmakta ve her tehdit her bir sunucu (veya servis) üzerinde önemli bir risk oluşturmaktadır.
- Yapılan bütün saldırılar eğer bir güvenlik önlemi yok ise başarılı sayılmaktadır.
- Yapılan saldırılar güvenlik cihazları tarafından gerçek zamanlı tespit edilip, durdurulabilecektir.

Oynanan oyunun modeli statik eksik bilgili işbiriksiz sıfır toplam olmayan tipindedir. Saldırgan ve savunan ortaklaşa çalışmayacaklarından dolayı işbiriksiz bir oyundur. Saldırgan ve savunan kendi hareketlerini yaptıklarında, saldırı ve savunma stratejilerinin bir genel maliyeti olacak, bu yüzden karakteristik fonksiyonu sadece kazançları hesaplayarak bir sonuç gösteremeyecektir. Kısacası birinin karı her zaman diğerinin %100 kazancı olmamaktadır. Bu yüzden oyun sıfır olmayan toplam tipli bir oyundur.

Saldırganın kazancı, sistemin kaybettiği değerin belli bir yüzdesi kadar olmaktadır. Bu modelin asıl amacı, bulut sağlayıcıdan alınan kaynakların içinde bulunan veya içine kurulan sistemlere karşı oluşturabilecek bir saldırı sonucunda savunana seçebileceği savunma stratejileri sunmaktır.

Tanım1: $G: (P, S, U)$

- a. $P = (1, 2, \dots, n)$ saldıran ve savunan tarafındaki oyuncuları göstermektedir.
- b. $S = (s_1, s_2, \dots, s_n)$ strateji uzayını göstermektedir ve $\forall x \in P$, $S_x \neq \emptyset$,
 $S_x = (s_1^x, s_2^x, \dots, s_m^x)$ x oyuncusunun strateji kümesidir.
- c. $U = (U_1, U_2, \dots, U_n)$ oyuncuların karakteristik fonksiyonlarıdır.

Tanım2: Önerilen model iki oyunculu statik sonlu işbirliksiz sıfır olmayan toplam tipinde olmaktadır:

$$\text{BBGOTM} = (\{a, d\}, \{S_a, S_d\}, \{U_a, U_d\})$$

Burada a saldırganı, d ise savunanı göstermektedir. Saldırganın strateji uzayı $S_a = (s_1^a, s_2^a, \dots, s_n^a)$, s_i^a ise bir saldırı stratejisi olmaktadır. Savunanın strateji uzayı $S_d = (s_1^d, s_2^d, \dots, s_n^d)$, s_i^d ise savunanın bir stratejisi olmaktadır. U_a ve U_d ise saldırgan ve savunanın karakteristik fonksiyonlarını belirtmektedir.

3.1. SALDIRI MODELLEMESİ

Ağ güvenliği alanında yapılan çalışmalarda (MIT Lincoln Laboratuvarı [17] Saldırıları) saldırıların sunucular üstündeki etkileri tam olarak bir parametre ile ifade edilememektedir. Bu etkileri belirlemek için günümüz güvenlik dünyasından temel olarak bilinen GBE (Gizlilik, Bütünlük, Elde edilebilirlik) kavramı kullanılacaktır. Bir saldırı sonucunda sunucunun üstündeki etki bu kavramlar ile hesaplanabilir. Saldırıların sınıflandırılmasında temel olarak yapılan saldırının tipi ile ne elde edilmek istendiği ve saldırının stratejik hedefleri değerlendirilmiş ve buna göre her özelliğe 0 ile 1 arasında puan verilmiştir (tablo 3.1).

Tablo 3.1 - Örnek Saldırı Sınıflandırması

Kategori	Tanım	Gizlilik	Bütünlü.	Elde Edile.
DoS	Dağıtık hizmet engelleme	0	0	1
Kullanıcı	Kullanıcı yetkisi kazanma	0,5	0,1	0,05
Veri	İzinsiz veri yazma ve okuma	1	1	0,2
Yönetimsel	Yönetici yetkisi edinme	1	0,1	0,05
Tarama	Tarama saldırısı	0,3	0	0,2

Savunma metotlarını ise savunma işleminin harcadığı zamana ve yapılan işlemin sisteme etkisine göre tablo 3.2'de gösterildiği şekilde üçe ayrılmıştır.

Tablo 3.2 - Örnek Savunma Sınıflandırması

Kategori	Tanım	Özellikler
Basit	Sanal makine ayarlarının değiştirilmesi	Gerekli işlem için harcanan zaman az ve sistemin durdurulmasına gerek yok
Orta Seviye	Yeniden başlatma, yönetici yetkisi kullanılarak ayar değiştirilmesi, politika değiştirilmesi, güvenlik güçlendirilmesi	Gerekli işlem için harcanan zaman daha uzun, profesyonel bilgi gerekli, sistem gerekirse durdurulabilir
İleri Seviye	Sistem yedeği alma, sanal güvenlik ürünleri kurma veya güncelleme, sistem güncellemesi, virüs taraması	İşlem çok uzun sürmekte, profesyonel bakım gerektirir ve sistem tamamıyla kapatılabilir.

3.2. SİSTEMİN DEĞERİNİN HESAPLANMASI

Bulut bilişimi bulut bilişim yapan asıl şey sanallaştırmadır. Sanallaştırma bir donanımın (işlemci, ram, vb.) sanal bir sürümünü yaratmaktır. Temelde sanallaştırma bir varlığın daha verimli kullanılabilmesi için birden fazla sanal varlıklara bölünmesidir. Örnek olarak gününüzde tek bir servis veren sunucuların işlemcilerinde genellikle %20'lik bir yük görülmektedir. Geri kalan %80'lik kısım

ise çöpe gitmektedir. Eğer bu işlemci 5'e bölünüp, her işlemciye diğer sunuculardan aynı işi bir görev verilir ise, işlemcinin kullanımı %100 yakın bir değere yaklaşır.

Üzerinde çalışılan sistemin fiziksel makine üzerinde çalışan bir sanal makine olarak görülmesi bu sistemin değerini belirlemek istendiğinde birden fazla şeyin daha dikkate alınmasına neden olmaktadır. Bu şeylerden biri canlı göç (live migration) yöntemidir. Canlı göç, bir sistemin bir fiziksel konumdan başka bir fiziksel konuma verilen hizmeti aksatmadan yapılan taşıma işlemidir. Canlı göçün yapılma nedenleri arasında yük dengeleme, verimi artırma ve saldırı altındaki sistemleri koruma olarak bulunmaktadır.

Önerdiğimiz yöntem, incelenen etkenden bir saldırı sonucu etkileneceği gizlilik, bütünlük ve elde edilebilirlik değerlerini istemektedir. Bu değerlerin canlı göç dikkate alındığında sabit kalmayacağı görülmektedir. Her canlı göç, fiziksel ve sanal sunucuların varlık olarak değerlerini değiştirmektedir.

Bu durum, belirli aralıklarla sunucuların gizlilik, bütünlük ve elde edilebilirlik değerlerini bir veri tabanında saklanarak çözülebilir. Yeni bir sanal sistem yaratıldığında, servisi satın alanın ihtiyacına ve bulut sağlayıcının politikalarına göre bir GBE değeri belirlenir. Böylece, sistem bulut altyapısına salındığı anda önemine göre bulut sağlayıcı tarafından verilen bir değeri bulur. Ne zaman bu sistem başka bir sisteme göç yaparsa, sistemin GBE değeri göç ettiği fiziksel konumdaki diğer sanal sistemlere bağlı olarak değişecektir. Bu değişen verilerin veri tabanı üzerinde saklanmasıyla, bu sistemin zaman içinde değişen değerine göre önemi belirlenebilir.

Oluşturulan veri tabanının büyümesi bulut bilişimin büyüklüğü dikkate alındığında çok hızlı olacaktır. Bu hızlı büyüme sorununu çözmek için Round Robin veri tabanı [18] saklama yöntemi kullanılabilir. Round Robin veri tabanı aracını belli bir aralıktaki noktaların ortalamasını alır ve bu aralığı tek bir noktaya düşürür. Örneğin bir veri 1 yıllık bir veri ise, bir yıl öncesine bağlı her gün alınan data değil de haftalık ortalama yeterli olabilir. Böylece 7 adet veri noktası, tek bir veri noktasına düşürülür. Yani, verinin güncelliği bir seneyi geçince, verinin doğruluğu azalmaktadır fakat bu veriden hala yeterli bilgi sağlanabilmektedir. Doğal olarak hiç veri olmamasından daha iyidir.

3.3. RİSKLERİN KARŞILAŞTIRILMASI

Önerilen model ile risklerin birbirleri arasında karşılaştırması bazı modellerden farklı olarak nicel şekilde yapıldığından dolayı, riskler arasında sayısal bir karşılaştırma aşağıdaki gibi yapılabilmektedir:

- Saldırı sınıflandırması göz önüne alındığında sunucunun zarar alabileceği özellikleri gizlilik, bütünlük ve elde edilebilirliğin (V_C, V_I, V_A),
- Saldırının aynı özelliklerdeki zarar verme seviyeleri ile çarpılması (L_C, L_I, L_A) ile beraber,
- Ulusal Güvenlik Açığı Veri Tabanı [19] üzerindeki ilgili açıklığa ait etki ortanı [20] ile çapılır (E_{fac}).

$$\text{Riskin Sistem Üzerinde Etkisi} = E_{fac} * ((L_C * V_C) + (L_I * V_I) + (L_A * V_A)) \quad (1)$$

Bu şekilde elde edilen sayısal değerler, var olan sistem üzerinde oluşabilecek risklerin tek tek hesaplanması sonucunda birbirleri arasında karşılaştırılabilir. Ayrıca aynı riskleri içinde barındıran farklı bulut servis modelleri (SoY, SoP, SoA vb.) arasında da bu riskler karşılaştırılabilir. Örnek olarak, 1, 2, 3, 4, 5 şeklinde riskler tanımlanırsa, SoY üzerinde bu risklerin vereceği hasarlar büyüklüğe göre 3, 4, 5, 2, 1 olurken, SoP üzerinde aynı risklerin vereceği hasarlar büyüklüğe göre 4, 5, 2, 3, 1 şeklini alabilir.

3.4. KAZANÇ TABLOSUNUN HESAPLANMASI

U_{kl}^a 'yi saldırganın karakteristik fonksiyonu olarak kabul edersek, B_{kl}^a saldırganın saldırıdan kazandığı kazanç, C_{kl}^a ise saldırının maliyeti olmaktadır. k ve l simgeleri ise saldırganın k stratejisini ve savunanda l stratejisini seçtiğini gösterir. Aynı şekilde U_{kl}^d savunanın karakteristik fonksiyonunu, B_{kl}^d savunanın kazancını, C_{kl}^d ise savunanın maliyetini belirtmektedir. k ve l simgeleri ise saldırganın k stratejisini ve savunanda l stratejisini seçtiğini gösterir.

Tanım 3: Katılan oyuncuların karakteristik fonksiyonları:

$$U = B - C \quad (2)$$

Yani, saldırganın karakteristik fonksiyonu

$$U_{kl}^a = B_{kl}^a - C_{kl}^a \quad (3)$$

olmaktadır. Savunanın ise

$$U_{kl}^d = B_{kl}^d - C_{kl}^d \quad (4)$$

olmaktadır.

3.5. SAVUNMANIN KAZANCI

Saldırı sınıflandırmasına göre bir sunucunun gizlilik, bütünlük ve elde edilebilirlik özellikleri hasar görmektedir. Bu sunucuya verilen hasarın seviyesi L_C, L_I, L_A şeklinde ve bu sunucunun değeri de aynı cinsten V_C, V_I, V_A şeklinde belirtilirse, bu değerlerin çarpımı sunucunun kaybettiği değer olmaktadır.

Tablo 3.3 - Savunmanın Kazancı

Strateji	Kazanç
s_k^a, s_l^d	$B_{kl}^d = (R_C - L_C) * V_C + (R_I - L_I) * V_I + (R_A - L_A) * V_A$
$s_k^a, -s_l^d$	$B_{kl}^d = -((L_C * V_C) + (L_I * V_I) + (L_A * V_A))$
$-s_k^a, s_l^d$	$B_{kl}^d = 0$
$-s_k^a, -s_l^d$	$B_{kl}^d = 0$

Eğer sunucu geri kurtarılır ise, R sunucu kurtarıldığında GBE sınıflandırmasında geri kazanılan değer olarak kabul edilmektedir:

$$Geri\ Kazanılan\ Sunucu\ Değeri = (R_C * V_C) + (R_I * V_I) + (R_A * V_A) \quad (5)$$

Tablo 3.3'te gösterilen $s_l^d s_k^a$ saldırı stratejisine karşı başarılı savunma strateji olmaktadır. $-s_l^d$ ise s_k^a saldırı stratejisine göre başarısız savunma stratejisi olmaktadır. $-s_k^a$ ise saldırının uygulanmadığı belirtmektedir.

3.6. SAVUNMANIN MALİYETİ

Savunanın aldığı güvenlik önlemlerinin maliyeti olacaktır. Bu maliyetler yapılan sınıflandırmaya göre farklı değerler almaktadır.

Temel olarak maliyetler üç adettir:

- Operasyon Maliyeti (C_O): Harcanan zaman ve hesaplama kaynakları
- Sunucu Geri Kazanım (C_R): İşlem için harcanan masraflar (maddi maliyet)
- Sistem Kullanılabilirliği (C_A): Sistemin kapatılmasından doğan masraflar (zararlar)

Operasyon maliyeti alınacak güvenlik önlemlerinin yaratacağı zaman ve bilgisayar kaynakları üzerindeki ekstra getireceği yükü belirtmektedir. Sunucu geri kazanım ise aynı sağlayıcı üzerinde barınan ve daha önce saldırı altında kalmış sistemlerin kurtarılmasında harcanacak maddi maliyeti temsil etmektedir. Bazı güvenlik önlemlerinin uygulanabilmesi için sistemin kapatılması veya yeniden başlatılması gerekebilir. Bu durumun elde edilebilirlik özelliğine etkisi sistem kullanılabilirliği altında ele alınmıştır. Tablo 3.4’de savunmanın güvenlik önlemi aldığı zaman ödeyeceği masraflar gösterilmiştir.

Tablo 3.4 - Savunmanın Maliyeti

Strateji	Masraflar
s_k^a, s_l^d	$C_{kl}^d = C_O + C_R + C_A$
$s_k^a, -s_l^d$	$C_{kl}^d = 0$
$-s_k^a, s_l^d$	$C_{kl}^d = C_O + C_R + C_A$
$-s_k^a, -s_l^d$	$C_{kl}^d = 0$

3.7. SALDIRGANIN KAZANCI

Saldırganın kazancı savunma sisteminin kaybı olmaktadır. Yani sunucu veya sistemin değer kaybıdır. Fakat GBE değerlendirmesinde kaybedilen her değer, tam olarak saldırgan tarafından kazanılmayabilir. Bu yüzden $z \in [0,1]$ kaybedilen

değerin ne kadarının saldırgan tarafından kazanıldığı gösteren bir değer olarak tanımlar isek, saldırganın kazancı

$$B^a = -k * B^D \quad (6)$$

olmaktadır. Tablo 3.5’de saldırganın saldırdığı zaman aldığı kazanlar gösterilmiştir.

Tablo 3.5 - Saldırganın Kazancı

Strateji	Kazanç
s_k^a, s_l^d	$B_{kl}^a = k((R_c - L_c) * V_c + (R_l - L_l) * V_l + (R_A - L_A) * V_A)$
$s_k^a, -s_l^d$	$B_{kl}^a = k((L_c * V_c) + (L_l * V_l) + (L_A * V_A))$
$-s_k^a, s_l^d$	$B_{kl}^a = 0$
$-s_k^a, -s_l^d$	$B_{kl}^a = 0$

3.8. SAVUNMANIN MALİYETİ

Saldırgan saldırıyı yapabilmesi için gerekli aletlere sahip olması ve saldırı için ihtiyaç duyulan zaman saldırının operasyon maliyetini C_{AO} belirtir. Ayrıca saldırı savunan tarafından tespit edilirse, saldırgan kendini ifşa ettiğinden dolayı bir ceza bedeli C_D ödemektedir. Tablo 3.6’da saldırganın yakalandığı zaman ödeyeceği masraf ikinci satırda (s_k^a, s_l^d stratejisi) ve eğer gerekli önlem savunan tarafından alınmamış ise, saldırganın saldırıyı yapması için gereken masraflar ise üçüncü satırda ($s_k^a, -s_l^d$ stratejisi) gösterilmiştir.

Tablo 3.6 - Saldırganın Maliyeti

Strateji	Masraflar
s_k^a, s_l^d	$C_{kl}^a = C_{AO} + C_D$
$s_k^a, -s_l^d$	$C_{kl}^a = C_{AO}$
$-s_k^a, s_l^d$	$C_{kl}^a = 0$
$-s_k^a, -s_l^d$	$C_{kl}^a = 0$

4. UYGULAMA ÖRNEĞİ VE DEĞERLENDİRME

Önerilen yöntemi tanıtılması için iki farklı bulut sağlayıcının kullandığı farklı hizmet modelleri etrafında bir senaryo oluşturulmuştur. Deney içinde bulunan bulut sağlayıcılardan alınan kaynakların kullanım amacının veri tabanlarıyla ilgili bir iş olduğu varsayılmıştır.

Bu deneyde bulut içinde bulunan veri tabanı sunucularının değerleri Tablo 4.1’de gösterilen şekilde alınmıştır.

Tablo 4.1 - Farklı Servis Modellerindeki Sunucuların Varlık Değerleri

	Gizlilik	Bütünlük	Elde Edilebilirlik
SoY VT	100	100	60
SoA VT	20	80	100

Servis olarak yazılım modeli içinde bulunan veri tabanı sunucusunda, bulut sağlayıcı sunucunun bütünüün güvenliğinden sorumlu iken (bkz. tablo 2.1), servis olarak altyapı sağlayan bulut sağlayıcı ise sadece sunucunun mevcut olma güvenlik özelliğinden sorumlu olmaktadır. Bu yüzden dolayı iki farklı hizmet modelinde aynı sunucu farklı varlık değerlerine sahiptir. Burada unutulmaması gereken önemli bir nokta ise, bir SoA sistemin üstüne SoY sistem kurulabilmesidir. Yani bir SoY firması gerekli altyapıyı SoA hizmeti veren bir bulut sağlayıcısından alabilmektedir. Bu durumda güvenliğin büyük kısmı SoY hizmeti veren firma veya SoA hizmetini satın alan kullanıcı üzerine düşmektedir.

4.1. RİSK KARŞILAŞTIRMA

Farklı servis modellerindeki önemlilik derecesini görmek için beş farklı risk farklı servis modelleri üzerinde karşılaştırıldı. Bu riskler bulut üzerindeki bir sistemi etkileyecek gerçek açıklıklar arasından seçildi. Bu senaryo için tablo 3.1 üstündeki GBE hasar seviyeleri örnek alındı. Kullanılan gerçek dünya açıklıklarının tipleri:

- **CVE-2012-1820:** Bu açıklıkta Quagga yönlendirme programında bulunan bir hatadan dolayı uzaktan erişen saldırgan DoS saldırısı yapabilmektedir [21].

- **CVE-2012-2752:** VMware vMA 4.x ve 5.x sürümlerinde bir truva atı kütüphanesi ile o an çalışan klasörde kullanıcı yetkileri kazanılmaktadır [22].
- **CVE-2012-4579:** Çapraz kod çalıştırma yöntemi ile phpMyAdmin 3.5.x versiyonları üzerinde uzaktan erişen kullanıcılar tablolar ve tablo içindeki veriler üzerinde değişiklikler yapabilmekteydiler [23].
- **CVE-2011-4005:** Çapraz istek sahteciliği ile Cisco Small Business tipli yönlendiricilerin bazı firmware versiyonlarında admin yetkileri ile keyfi komutlar çalıştırılabilir [24].
- **CVE-2010-1638:** Horde (web üzerinden çalışan bir e-posta ara yüzü) üzerinde bulunan IMP eklentisi uzaktan erişen saldırganların güvenlik duvarı kısıtlamalarını aşmalarına izin vermektedir. Bu şekilde saldırgan Horde ara yüzünü vekil bir sunucu şeklinde kullanarak iç ağları taramakta kullanabilmektedir. [25]

Tablo 4.2 - Risklerin Hesaplanan Etkisi

Saldırı Tipi	SoY Puan Toplamı	SoA Puan Toplamı
DoS	330	550
Kullanıcı	245,7	89,7
Veri	1441,6	326,4
Yönetimsel	971,8	283,8
Tarama	420	80

Hesaplamaların sonucu tablo 4.2’de gösterilmiştir. Tabloya bakıldığında görüleceği gibi SoY modeli için risklerin önem sırası SoA’dan farklı olmaktadır. SoY hizmet modelinde veri ve yönetimsel saldırıların önemi diğerlerinden daha ön plana çıkmaktadır. Risk önem sırası veri, yönetimsel, tarama, DoS ve kullanıcı şeklinde olmaktadır. Fakat SoA hizmet modelinde DoS ve veri saldırıları daha önemli olmaktadır. Bunun nedeni SoA hizmet modeli alt yapı hizmeti vermekle sorumlu olmasıdır. Alt yapı üzerinde bulunan veya işlenen verilerin herhangi bir durum altında çalınması kullanıcının sorumluluğundadır. SoA hizmet modeli için risk önemlilik sırası ise DoS veri, yönetimsel, kullanıcı ve tarama olmaktadır.

4.2. RİSK OYUNU

Sunucular üstünde risk karşılaştırmasında kullanılan açıklardan farklı bir açıklık ele alınmıştır. Sunucular üstünde CVE-2012-0116 [26] açıklığı bulunduğu varsayılmıştır. Bu açıklık MySQL veri tabanına uzaktan bağlanan kullanıcıların gizlilik ve elde edilebilirlik özelliklerine etkilemesine izin vermektedir. Bu açıklığa uygun saldırı modeli tablo 3.1’de yer alan veri kategorisinde bulunan izinsiz veri yazma ve okuma olarak seçilmiştir. Bu saldırının vereceği hasar seviyeleri sırayla $L_C = 1$, $L_I = 1$, $L_A = 0,2$ olmaktadır. Bazı parametreler deneyimlere bağlı olarak verilmiştir: $R_C = 1$, $R_I = 1$, $R_A = 0,4$.

Açıklığı gidermek için gereken işlemin maliyeti ise sırayla $C_O = 60$, $C_R = 70$, $C_A = 50$ olmaktadır. Saldırının işlem maliyeti ise $C_{AO} = 30$ olmakta ve saldırgan tespit edildiği zaman ise $C_D = 50$ ceza ödemektedir.

Tablo 4.3 - SoY Veri Tabanı Sunucusu Çözüm Matrisi

	Savun	Önlem Alma
Saldırı Yap	-92, -168	194, -224
Eylem Yapma	0, -180	0,0

Açıklığı gidermek için gereken işlemin maliyeti ise sırayla $C_O = 60$, $C_R = 70$, $C_A = 50$ olmaktadır. Saldırının işlem maliyeti ise $C_{AO} = 30$ olmakta ve saldırgan tespit edildiği zaman ise $C_D = 50$ ceza ödemektedir.

Saldırının ve savunanın karakteristik fonksiyonları hesaplandıktan sonra ortaya çıkan sonuç matrisleri tablo 4.3 ve tablo 4.4’de gösterilmiştir.

Nash dengesine göre, her sonlu oyunda en az bir denge noktası bulunmaktadır. Tablo 4.4’de gösterilen SoA matrisinin tanımladığı oyunu oyuncuların birbirlerinin oynadığı hareketlere verebilecekleri en iyi cevapları göstererek çözebiliriz. Eğer saldırgan saldırıyı gerçekleştirir ise, savunanın önlem almaması kendi çıkarı açısından daha iyi sonuç vermektedir. Eğer savunan önlem almaz ise, saldırganın kendi çıkarı açısından saldırması saldırmamasına göre daha iyi sonuç vermektedir. Bu yüzden dolayı matrisin sağ üst kısmı Nash dengesidir.

Tablo 4.4 - SoA Veri Tabanı Sunucusu Çözüm Matrisi

	Savun	Önlem Alma
Saldırı Yap	-100, -160	110, -140
Eylem Yapma	0, -180	0,0

Bu tip oyunlarda ya katkısız strateji Nash dengesi veya karma Nash dengesi bulunmaktadır. SoY çözüm matrisinde ise SoA çözüm matrisindeki gibi katkısız strateji Nash dengesi bulunmamaktadır. Karma Nash dengesi SoY matrisi uygulandığında, savunanın 0,68 olasılıkla savun seçeneğini seçmesi saldırganın saldırı yap ve saldırma seçeneklerinin bedelleri eşitlemektedir. Bu yüzden saldırgan saldırıya da saldırmasa da aynı bedeli almaktadır. Aynı şekilde saldırgan 0,79 olasılıkla saldırı gerçekleştirir ise, savunanın güvenlik önlemi alması ve alması arasında bir bedel farkı bulunmamaktadır.

Kısacası eğer savunan kişi elindeki sistemlerin %68'inin üzerinde güvenlik önlemi aldığı takdirde, saldırgan saldırmadığı takdirdeki bedeli saldırdığı takdirdeki ödediği bedelden fazla olmaktadır. Elde edilen bu sonuç savunmanın güvenlik önlemlerini planlamasında kullanılabilecektir.

Önerilen modelin diğer yöntemlere göre üstün yanı, varlığa verilen değere göre ve varlığın vereceği hizmete göre güvenlik önlemleri alınabilmesidir. Böylece bulut bilişimde farklı hizmet modellerinde, o sistemin güvenliğinden sorumlu şahıs veya kuruluşlar sorumlu oldukları alan kadarı ile güvenlik önlemi almaktadır. Kısaca, bulut bilişimde hizmet modellerinin gerektirdiği ihtiyaçlara göre ve kullanan şahıs veya kurumların isteklerine göre ölçeklendirilebilir güvenlik sağlanmaktadır. Bütün sistem üzerinde uygulanacak ve uzun sürecek ve güvenlik değerlendirme yöntemi kısaltılmakta ve dinamikleştirilmektedir.

Önerilen yöntem FPVA (First Principles Vulnerability Assessment) [13] yöntemi gibi el ile büyük bulut uygulama programla ara yüzlerine bakan sistemlerden daha hızlı alışmaktadır. FPVA ayrıca her düğüm noktasını incelemeyi dener, fakat önerilen yöntem seçici denetim yaparak gelecek saldırıyı tahmin eder. Risk değerlendirme yöntemi SEBCRA (Semi-quantitative BLO (Business-level objectives) driven Cloud Risk Assessment) [15] yönteminden daha geniş bir açıya bakmaktadır. SEBCRA yönteminde hizmet seviyesi sözleşmesi gibi ihlali gibi bazı

olaylar yararlı etkileri olduğu dikkate alınmaktadır. Fakat gelecekte bu durumun riske dönüşebileceği düşünülmemektedir. Bu nedenle önerilen yöntemde olaylar hiçbir zaman yararlı olay olarak ele alınmamıştır. Yöntemin bir başka önemli noktası ise, bazı diğer yöntemler [16] aksine, alınabilecek güvenlik önlemleri servis modeline göre seçilebilmektedir. Kısacası, gerekli güvenlik önlemleri kişilerin veya kurumların isteklerine göre uygulanabilmektedir.

Risk değerlendirmede kullanılan en yaygın ölçütlerden biri yıllık kayıp beklentisidir (ALE). Bu değerlendirme riskin bir yıl içinde oluşma sıklığı ile maliyetinin çarpımı sonucu elde edilir. Bir varlığın yıllık kayıp maliyeti:

$$ALE = SLE \times ARO \quad (7)$$

formülü ile hesaplanır. ARO değeri bir yıl içinde oluşma sıklığını temsil etmekte iken SLE ise varlık için parasal kayıp beklentisidir. SLE değeri:

$$SLE = Varlık Değeri \times Maruz Kalma Faktörü \quad (8)$$

şeklinde hesaplanır. Maruz kalma faktörü, varlığın risk altında kaldığı anda kaybedeceği maddi değer yüzdesi olarak karşılığı olmaktadır. Örneğin 5000 TL'lik bir mal, riskin gerçekleşmesi sonrasında %10 kayıp veriyor ise :

$$SLE = 5000 \times 0,10 = 500 TL \quad (9)$$

şeklinde kayıp yaşanacaktır.

Sunulan senaryoda tablo 4.3'de verilen örnekte sistemin %68'nin korunması saldırganın saldırı yapması ile yapmama şansını eşitlemektedir. Burada sistemin korunmayan %32'lik kısım parasal kayıp beklentisi formülünde kullanılabilir. Bir saldırı oluşur ise, sağlayıcının korumadığı kısımdan kaybettiği maliyetin, bu kısmı korumak için alınacak güvenlik sisteminin masrafının altında mı üstünde mi olduğu değerlendirilerek, gerekirse geri kalan kısımlarda korunma altına alınabilir.

5. SONUÇ VE ÖNERİLER

Bulut bilişimin birçok avantajının bulunmasına rağmen herkes için uygun bir çözüm olmadığı anlaşılmaktadır. Kritik uygulamaların bulut bilişime şu an geçmesi bir risk oluşturmaktadır. Özellikle yasalar banka gibi bazı kurumların bulut bilişim kullanmasına izin vermemektedir. Bir başka önemli nokta ise bulut bilişim piyasada bulunan az bilgili sistem ve ağ mühendislerini piyasadan temizleyecektir.

Bulut bilişim getirdiği birçok avantajın yanı sıra, birçok güvenlik problemini de birlikte getirmektedir. Bu güvenlik problemleri yönetilmesi ve değerlendirilmesi günümüz yöntemleri ile yapılması yetersiz kalmaktadır. Bunun yanı sıra şu an bilinmeyen fakat gelecekte gerçekleşebilecek açıklıklara karşı bir önlem günümüz yöntemleri ile alınamamaktadır.

Bu çalışmada bulut bilişim sistemlerinde bulunan güvenlik sorunları ele alınmıştır. Geleneksel bilgi teknolojileri sistemleri ile bazı sorunları paylaşmakta olsa da, bulut bilişim birçok noktada geleneksel bilgi teknolojileri sorunlarına getirilen çözümleri bir değişiklik uygulamadan kullanılamamaktadır.

Günümüz yöntemleri bulut bilişimde saldırgan ve savunanın kazançlarını ve masraflarını ön plana çıkarmamaktadır. Bu çalışma, bulut bilişim kullanılması durumunda ideal güvenlik önlemlerinin bulunmasında yardım etmektedir. Önerilen modelde ekonomide çok sık kullanılan oyun teorisi kullanılarak saldırgan ve savunanın çıkar modellemesi yapılmıştır. Savunanın ideal güvenlik stratejisi sunucu değerlerine ve sunucu üstündeki saldırı risklerine bakılarak hesaplanmıştır. Bu model, sabit olarak sadece bulut bilişimdeki objelerin birbirleri ilişkilerine bakarak, aralarında oluşabilecek riskleri bulut bilişimin altyapısını oluşturan devasa kod üzerinde aramaktan daha hızlı ve verimli olmaktadır.

Saldırganın yapabileceği aynı tipteki saldırıları çözüm matrisinde farklı satırlara konarak ve buna karşı savunanın uygulayabileceği güvenlik önlemleri de farklı sütunlara konularak çözüm matrisinin büyütülmesi ile hangi güvenlik önleminin aynı tip birden fazla risk için daha verimli bir sonuç verdiği gelecekte yapılacak çalışmalar arasındadır. Bu şekilde ortaya çıkan matriste, saldırganın saldırılarından cayması için savunanın alınabilecek hangi güvenlik önlemlerinin hangi sistemin en azından ne kadarına uygulaması gerektiği hesaplanacaktır. Karakteristik fonksiyonun

oluşturan değişkenlerin bulut sağlayıcının geçmişinden öğrenerek, bulut sağlayıcının verdiği hizmet modeline uygun sonuçlar verebilmesi de gelecekte yapılacak çalışmalar arasındadır.

KAYNAKLAR

- [1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, 2011.
- [2] S. Eliot, "What The Heck Is Cloud Computing? – Another re-look, with Pretty Pictures," 2010. [Online]. Available: <https://blogs.msdn.com/b/seliot/archive/2010/03/04/what-the-heck-is-cloud-computing-another-re-look-with-pretty-pictures.aspx>.
- [3] Y. Korkmaz, «Bulut Bilişim: Türkiye İçin Fırsatlar,» TÜBİTAK, [Çevrimiçi]. Available: http://www.tubitak.gov.tr/tubitak_content_files/bilgiguvenligi/sunular/Korkmaz_Bulut_Bilisim.ppt.
- [4] S. Almula and C. Y. Yeun, "Cloud computing security management," *Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference*, pp. 1-7, March 2010.
- [5] Y. Korkmaz, «Bulut Bilişim Risk Değerlendirmesi - II,» Haziran 2010. [Çevrimiçi]. Available: <http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bulut-bilisim-risk-degerlendirmesi-ii.html>.
- [6] K. Craig-Wood, "IaaS vs. PaaS vs. SaaS definition," [Online]. Available: <http://www.katescomment.com/iaas-paas-saas-definition/>.
- [7] C. Hoff, "Dear Mr. Schneier, If Cloud Is Nothing New, Why Are You Talking So Much About It?," [Online]. Available: <http://www.rationalsurvivability.com/blog/2009/06/dear-mr-schneier-if-cloud-is-nothing-new-why-are-you-talking-so-much-about-it/>.
- [8] J. Pita, M. Jain ve J. Marecki, «Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International

Airport,» Estoril, Portugal, 2008.

- [9] I. Kantzavelou and S. Katsikas, "A game-based intrusion detection mechanism to confront internal attackers," vol. 29, no. 8, 2010.
- [10] D. Liu, X. Wang and J. Camp, "Game-theoretic modeling and analysis of insider threats," *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 75-80, 2008.
- [11] H. Otrok, M. Mehrandish, C. Assi, M. Debbabi and P. Bhattacharya, "Game theoretic models for detecting network intrusions," *Computer Communications*, vol. 31, no. 10, pp. 1934 - 1944, 2008.
- [12] B. Wang, J. Cai, S. Zhang and J. Li, "A network security assessment model based on attack-defense game theory," in *2010 International Conference on Computer Application and System Modeling (ICCASM)*, Taiyuan Shanxi, China, 2010.
- [13] J. A. Kupsch, B. P. Miller, E. Heymann and a. E. César, "First principles vulnerability assessment," *In Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, Vols. ACM, New York, NY, USA, pp. 87-92.
- [14] L. Peiyu and L. Dong, "The New Risk Assessment Model for Information System in Cloud Computing Environment," *Procedia Engineering*, vol. 15, pp. 3200-3204, 2011.
- [15] J. O. Fitó and J. Guitart, "Business-driven management of infrastructure-level risks in Cloud providers," *Future Generation Computer Systems*, vol. <http://www.sciencedirect.com/science/article/pii/S0167739X12001045>, Available online 25 May 2012.
- [16] M. Kiran, M. Jiang, D. J. Armstrong ve K. Djemame, «Towards a Service Lifecycle Based Methodology for Risk Assessment in Cloud Computing,» *Dependable, Autonomic and Secure Computing (DASC)*, pp. 449-456, Dec 2011.

- [17] "Massachusetts Institute of Technology Lincoln Laboratory," [Online]. Available: <http://www.ll.mit.edu/index.html>.
- [18] "Round Robin Database Tool - RRDtool," [Online]. Available: <http://oss.oetiker.ch/rrdtool/>.
- [19] "National Vulnerability Database," [Online]. Available: <http://nvd.nist.gov/>.
- [20] "CVSS v2 Vector Definitions," [Online]. Available: <http://nvd.nist.gov/cvss.cfm?vectorinfo&version=2>.
- [21] "Vulnerability Summary for CVE-2012-1820," [Online]. Available: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1820>.
- [22] "Vulnerability Summary for CVE-2012-2752," [Online]. Available: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2752>.
- [23] "Vulnerability Summary for CVE-2012-4579," [Online]. Available: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4579>.
- [24] "Vulnerability Summary for CVE-2011-4005," [Online]. Available: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4005>.
- [25] "Vulnerability Summary for CVE-2010-1638," [Online]. Available: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1638>.
- [26] "Vulnerability Summary for CVE-2012-0116," [Online]. Available: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0116>.
- [27] H. Uzuner, «Cloud Computing Bulut Bilişim,» 26 Aralık 2010. [Çevrimiçi]. Available: http://www.cozumpark.com/blogs/cloud_computing/archive/2010/12/26/cloud-computing-bulut-bili-im.aspx.
- [28] "CVE-2007-4496 - Arbitrary code execution on the host operating system via unspecified vectors," [Online]. Available: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4496>.

- [29] "CVE-2007-4993: Xen guest root can escape to domain 0 through pygrub," [Online]. Available: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4993>.
- [30] "CVE-2007-5497: Vulnerability in Xen Server could result in privilege escalation and arbitrary code execution," [Online]. Available: <http://support.citrix.com/article/CTX118766>.
- [31] "CVE-2008-2100: VMware Buffer Overflows in VIX API Let Local Users Execute Arbitrary Code in Host OS," [Online]. Available: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2100>.
- [32] "Vulnerability Summary for CVE-2007-0948," [Online]. Available: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0948>.
- [33] D. Zissis ve D. Lekkas, «Addressing cloud computing security issues,» *Future Generation Computer Systems*, cilt 28, no. 3, pp. 583-592.
- [34] I. Deyrup and S. Matthews, "Cloud Computing & National Security Law," The Harvard Law National Security Research Group, [Online]. Available: <http://www.law.harvard.edu/students/orgs/nsrc/Cloud.pdf>.
- [35] D. Basak, R. Toshniwal, S. Maskalik and A. Sequeira, "Virtualizing networking and security in the cloud," *SIGOPS Oper. Syst.*, December 2010.
- [36] N. Bryson and A. Joseph, "Generating consensus priority interval vectors for group decision-making in the AHP," *Journal of Multi-Criteria Decision Analysis*, vol. 9, no. 4, pp. 127-173, 2000.
- [37] T. Carroll and D. Grosu, "A Game Theoretic Investigation of Deception in Network Security," *Computer Communications and Networks*, no. Proceedings of 18th International Conference on ICCCN 2009, pp. 1-6, Aug. 2009.
- [38] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing 3.0.

- [39] European Network and information Security Agency, "Cloud Computing Security Risk Assessment".
- [40] A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia and M. Armbrust, "Above the Clouds: A Berkeley View of Cloud Computing," *Commun. ACM* 53,4, pp. 50-80, April 2010.
- [41] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," *NIST*.
- [42] E. Keller, J. Szefer, J. Rexford and R. B. Lee., "NoHype: virtualized cloud infrastructure without the virtualization," *SIGARCH Comput. Archit. News* 38, pp. 350-361, July 2010.
- [43] K. Kortchinsky, "Cloudburst: A VMware Guest to Host Escape Story," *Blackhat USA 2009*.
- [44] A. Lenk, M. Klems, J. Nimis, S. Tai ve T. Sandholm, «What's inside the Cloud? An architectural map of the Cloud landscape,» *In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, no. IEEE Computer Society, Washington, DC, USA, pp. 23-31.
- [45] H.-C. Li, P.-H. Liang, J.-M. Yang and S.-J. Chen, "Analysis on Cloud-Based Security Vulnerability Assessment," *IEEE International Conference on E-Business Engineering*, pp. 490-494, 2010.
- [46] T. Ormandy, "An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments," *Google, Inc*, 2007.
- [47] P. Dorey, A. Leite and Commentary, "Commentary : Cloud computing – A security problem or solution?," *Information Security Technical Report*, vol. 16, no. 3-4, pp. 89-96, August–November 2011.
- [48] N. Nisan, T. Roughgarden, È. Tardos and V. V. Vazirani, *Algorithmic game theory*, Cambridge University Press, 2007.

- [49] S. Ramgovind, M. Eloff ve E. Smith, «The management of security in Cloud computing,» *Information Security for South Africa (ISSA)*, pp. 1-7, 2010.
- [50] S. Shiva, S. Roy and a. D. Dasgupta, "Game theory for cyber security," in *In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10)*, ACM, New York, NY, USA, 2010.
- [51] S. Subashini and V. Kavitha, "Review: A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1-11, 2011.
- [52] D. Svantesson and R. Clarke, "Privacy and consumer risks in cloud computing," *Computer Law; Security Review*, vol. 26, no. 4, pp. 391-397, July 2010.
- [53] M. J. Osborne, *An Introduction to Game Theory*, Oxford University Press, USA, 2003.
- [54] H. Wu, Y. Ding, C. Winer and L. Yao, "Network security for virtual machine in cloud computing," *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference*, pp. 18-21, December 2010.
- [55] J. Yang and Z. Chen, "Cloud Computing Research and Security Issues," *2010 International Conference on Computational Intelligence and Software Engineering (CISE)*, pp. 1-3, December 2010.

ÖZGEÇMİŞ

Evrin FURUNCU 1988 yılında Muğla’da doğdu. İlkokul öğretimine Gölcük/Kocaeli’nde başlayıp Marmaris/Muğla’da tamamladı. Lise hayatını ise Antalya’da başlayıp, Gölcük/Kocaeli’nde tamamladı. 2006’da girdiği İzmir Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümünden, 2010 yılında onur derecesi ile mezun oldu. Bilgisayarlara sadece işi ve çalışmaları dışında hobisi olarak ta görmekte olan Evrim FURUNCU, eğitim hayatı boyunca çeşitli eğitim kurumlarında bilgisayar sistemleri konusunda destek verdi. Halen Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği anabilim dalında yüksek lisans eğitimine ve araştırma görevliliği görevine devam etmektedir.