# Oyun Teorisi Kullanılarak Bulut Bilişimde Ölçeklendirebilir Güvenlik Değerlendirmesi

Evrim Furuncu, İbrahim Soğukpınar

*Özet*—**"Bulut Bilişim" günümüz Internet dünyasında ön plana çıkan kavramların başında gelmektedir. Bulut bilişim alt yapısında bulunan hizmet modellerinde uygulanan güvenlik, hizmet modellerine göre farklılıklar göstermektedir. Bir modelde uygulanan güvenlik diğer modelde farklı kişi veya kuruluşlara aktarılmakta, bu yüzden bir karmaşa yaşanmaktadır. Ayrıca bulut bilişim sistemi içindeki her varlık farklı güvenlik önlemi gerektirebilecektir. Bu husus, önemsiz bilgilerin yüksek güvenlik seviyesi ile saklanmasına neden olmakta ve bulut sağlayıcı gereksiz masraf yaşamaktadır. Bu çalışmada, ölçeklendirilebilir bulut bilişim güvenliği bu sorunlara çözüm olarak önerilmiştir. Bu çözüm günümüzde yaygın olan oyun teorisi ile dinamik olarak modellenmiştir.**

*Anahtar Kelimeler* — **Bulut Bilişim Güvenliği, Ölçeklendirebilir Güvenlik, Oyun Teorisi**

*Abstract* —**The term "Cloud Computing" is one of the most popular concepts of the today's IT world. The security of the service models in cloud computing is different from each other because of the infrastructure needed for each of the service models. The security implemented in a model is transferred to other persons or entities in a different model. This makes a mess about the security. Each asset in cloud computing may need the different security level as the other assets. This state causes unimportant information to have more security than needed and results in unnecessary expense. In this work scalable security in cloud computing has been proposed as a solution for this problem. This solution is presented by using one of the hot topics in today's dynamic security modeling, namely game theory. The game that is played in this problem is dynamic game with incomplete information, namely a Bayesian game.**

**Keywords— Cloud Computing Security, Scalable Security, Game Theory Security Modeling**

## I. GİRİŞ

Gelişen bağlantı hızları sayesinde uzaktaki güçlü sunucuların kaynaklarını verimli bir şekilde kullanarak işlerin yapılması, günümüzde bulut bilişim kavramını ortaya çıkarmıştır. İşletmeler bulut bilişimi kullanarak, bilgisayar kaynaklarının maliyetlerinde tasarruf ve esneklik elde edebilmektedirler. Talep üzerine kapasite ekleyerek, işletmeler bulut bilişimi kendi altyapılarını genişletme amacıyla kullanabilmektedirler.

Birden fazla kullanıcının ortak altyapı kullanması bu sistemin güvenliğini önemli kılmaktadır. Bulut bilişimin hizmet modelleri olan; SoY (Servis olarak Yazılım), SoP (Servis olarak Platform) ve SoA (Servis olarak Altyapı) modellerinin her birisinde farklı hizmetler belli bir kademeye kadar çalıştırılmaktadır. Mevcut hizmet modellerinde ihtiyaç duyulan farklı kaynaklar nedeniyle alınan güvenlik önlemleri de farklılık göstermektedir. Güvenlik önlemleri Bazı modellerde mutlaka alınması gerekirken, bazılarında alınması zorunlu olmamakta veya kullanıcının alması gerekmektedir. Bu önlemlerin servis modellerine göre değişiklik göstermesinin yanı sıra, bulut servis sağlayıcılar ile kullanıcılar arasında yapılan hizmet seviyesi anlaşmasına (SLA - Service-level agreement) göre de değişebilmektedir.

Tablo-1'de NIST tarafından bulut bilişim tanımında kullanılan [1] bulut servis modellerindeki güvenlik ihtiyaçları verilmiştir. Burada dikkat edilmesi gereken bir konu, bulut servis modellerinin sadece bu tanımdaki gibi üç modelden oluşmamasıdır. SoY, SoA ve SoP gibi modellerin yanında günümüzde hareketli operatörlerin kullandığı SoaA (Servis olarak ağ), yedekleme veya tekil kişilerin kullandığı SoDA (Servis olarak Depolama Alanı) ve işyerlerinin elemanlarının bilgisayarlarını buluta aktaran SoM (Servis Olarak Masaüstü) gibi modellerde gelişmektedir. Bu modellerin güvenlik gereksinimleri ihtiyaç duydukları kaynaklara göre değişmektedir. Örneğin SoaA'da mevcut olma gereksinimi diğer bütün gereksinimlere göre daha önemlidir. Bunun nedeni bu sistemin asıl kullanım amacı kullanıcıya ağı sunmak yani bant genişliği sağlamaktadır. Üzerinden geçen bilginin gizliliği, bütünlüğünün sağlanması servis sağlayıcıya ait değildir. Fakat servis olarak yazılım hizmetinde yapılan tüm işler bulut sağlayıcı tarafından yapıldığından dolayı, bulut sağlayıcı Tablo-1'de gösterilen her güvenlik özelliğini düşünmek ve uygulamak zorundadır.

| **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 1- Bulut bilişim güvenlik gereksinimleri

Evrim FURUNCU, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği, Gebze Yüksek Teknoloji Enstitüsü İstanbul Caddesi, P.K. 141,Gebze, 41400– Kocaeli, TÜRKİYE, Ttel: +90 262 605 22 32Fax: +90 262653 84 90 E-mail: efuruncu@bilmuh.gyte.edu.tr

İbrahim SOĞUKPINAR, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği, Gebze Yüksek Teknoloji Enstitüsü İstanbul Caddesi, P.K. 141, Gebze, 41400 – Kocaeli, TÜRKİYE, Ttel: +90 262 605 22 01Fax: +90 262653 84 90 E-mail: ispinar@bilmuh.gyte.edu.tr

Genel olarak ağ saldırganları zeki ve mantıklı insanlardır. Yapacakları saldırıların masraflarını ve kazançlarını göz önünde bulundururlar. Savunanlar ise saldırıyı engelleyerek bir kazanç sağlamakta, fakat herhangi bir saldırı olmadığı zamanda aldıkları güvenlik önlemlerinin bir maliyeti olmaktadır. Belirtilen özellikler bu durumun oyun teorisi tarafından modellemesini 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 için bir model önerilmiştir. Yöntemin kullanılmasıyla ortaya çıkan sonuca göre saldırgan veya savunanın kendi kârını artırarak 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.

Makalenin 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.

## II. BİLGİ GÜVENLİĞİNDE OYUN TEORİSİ VE İLGİLİ ÇALIŞMALAR?

Bilişim teknolojisi güvenliğinde saldırı, saldırgan ile hedef alınan sistemi güvenli yapan savunma sistemi arasındaki etkileşimdir. Savunma sistemleri ve saldırgan aktif oyuncular olmakta iken, hedef alınan sistem ise bütünün basit bir parçası olarak kalmaktadır. Etkileşimli sistemleri inceleyen çalışma oyun teorisidir. Bilişim teknolojisinde güvenlik bir oyunun özelliklerini taşımaktadır. Ekonomi, Biyoloji, Hukuk ve Psikoloji gibi bilimler oyun teorisi tekniklerini kullanmaktadırlar. Bilişim dünyasında ise nüfuz tespit sistemleri ve oyun teorisi çok çalışma yapılan konular arasındadır. Son yıllarda oyun teorisi, ekonomi teori ve bilgisayar bilimleri arasında yapılan çalışmalar Algoritmik Oyun Teorisi [10] alanına yön vermiştir.

Oyun teorisi modellemesinin amacı insanların neden belirli bir şekilde davrandığı ve bu davranışlara göre gelecekte yapacakları davranışlarını 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.

Güvenlik konusunda ise oyun teorisi, savunanın ve saldırganın belirli olasılıklarla seçeceği stratejilere göre, ideal savunma veya saldırı stratejisi seçilmesinde yardım etmektedir. 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.

Bulut bilişimde güvenlik değerlendirmesi yeni bir konu olduğundan dolayı bu konuda yapılan çalışmalar nispeten yenidir. Yapılan çalışmaların büyük bir kısmı ise sadece bilgisayar kümeleri teknoloji düşünülerek yapıldığından dolayı, bulut bilişimin en önemli yanı olan depolama güvenliği arka planda kalmakta ve genelde statik bir güvenlik değerlendirmesi önerilmektedir.

Kupsch, Miller, Heymann ve César önerdikleri modelde [5], bulut bilişimden daha çok ızgara hesaplama yapan sistemlerde program ile donanım arasında çalışan katmana uygulanmaktadır. 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[3]:

- Katman 1: İlk aşamada problem hiyerarşik bir düzende formülleştirilmektedir. En üst katman ulaşılacak 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 gerçekleştirilmesi 3 prensibe bağlıdır: Ayrıştırma, 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.

## III. Bulut Bilişim Güvenliğinin Oyun Teorisi Modeli(BBGOTM)

Güvenlik modellemesi yapılırken tehditlerin hesaplanması güvenlik değerlendirmesinin en önemli parçasıdır. Bu ihtiyaçlara göre aşağıdaki 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 işbirliksiz sıfır toplam olmayan tipindedir. Saldırgan ve savunan ortaklaşa çalışmayacaklarından dolayı işbirliksiz 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:** $\boldsymbol{G}: (\boldsymbol{P}, \boldsymbol{S}, \boldsymbol{U})$

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

### *A. Saldırı ve Savunmanın Modellenmesi*

Ağ güvenliği alanında yapılan çalışmalarda (MIT Lincoln Laboratuvarı 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.

| Kategori | Tanım | G | B | E |
|---|---|---|---|---|
| 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 |

Tablo 2 - Örnek Saldırı Sınıflandırması

Savunma metotlarını ise savunma işleminin harcadığı zamana ve yapılan işlemin sisteme etkisine göre Tablo 3'de gösterildiği şekilde üçe ayrılmıştır.

| 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 güçlendirmesi | 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. |

Tablo 3 - Örnek Savunma Sınıflandırması

### B. Kazanç Tablosu Hesaplaması

$U_{kl}^{a}$ '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 savunanında $l$ 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 savunanında $l$ stratejisini seçtiğini gösterir.

**Tanım 3:** Katılan oyuncuların karakteristik fonksiyonları:

$$U = B - C \quad (1)$$

Yani, saldırganın karakteristik fonksiyonu

$$U_{kl}^{a} = B_{kl}^{a} - C_{kl}^{a} \quad (2)$$

olmaktadır. Savunanın ise

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

olmaktadır.

### C. Savunanın Kazancı

Saldırı sınıflandırmasına göre bir sunucunun gizlilik, bütünlük ve elde edilebilirlik özellikleri hasar görmektedir. Bu

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

Tablo 4 - Savunanın Kazancı

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.

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

$$\textit{Geri Kazanılan Sunucu Değeri} = (R_C * V_C) + (R_I * V_I) + (R_A * V_A) \quad (4)$$

Tablo 4'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.

### D. Savunanın Maliyeti

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

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

Tablo 5 - Savunanın Maliyeti

• Sunucu Geri Kazanım ($C_R$): İşlem için harcanan masraflar (maddi maliyet)

• Sistem kullanılabilirliği ($C_A$): Sistemin kapatılmasından doğan masraflar (zararlar)

### E. Saldırganın Kazancı

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

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

Tablo 6 - Saldırganın Kazancı

$B^a = -k * B^D$ olmaktadır.

### F. Saldırganın Masrafı

Saldırgan saldırıyı yapabilmesi için gerekli aletlere sahip olması ve saldırı için ihtiyaç duyulan zaman saldırının operasyon maliyetini belirtir. Ayrıca saldırı savunan tarafından tespit edilirse, saldırgan kendini ifşa ettiğinden dolayı bir ceza

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

Tablo 7 - Saldırganın Maliyeti

bedeli ödemektedir.

## IV. UYGULAMA ÖRNEĞİ VE DEĞERLENDİRME

Güvenlik değerlendirmesi yöntemini tanıtmak için bir senaryo oluşturulmuştur. Bu senaryoda farklı iki modelde hizmet veren bulut sağlayıcıların içinde bulunan bir veri tabanı sunucu değerlendirilmiştir.

Bu deneyde bulut içinde bulunan veri tabanı sunucularının değerleri Tablo-8'deki gibi alınmıştır.

Servis olarak yazılım modeli içinde bulunan veri tabanı sunucusunda, bulut sağlayıcı sunucunun bütünün

güvenliğinden sorumlu iken (bknz. Tablo-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.

| | Gizlilik | Bütünlük | Mevcut Olma |
|---|---|---|---|
| **SoY VT** | 100 | 100 | 60 |
| **SoA VT** | 20 | 80 | 100 |

Tablo 8 - Farklı Servis Modellerindeki Sunucuların Varlık Değerleri

Sunucular üstünde CVE-2012-0116 [12] açıklığı bulunduğu varsayılmıştır. Bu açıklığa uygun saldırı modeli Tablo-2'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.

| | Savun | Önlem Alma |
|---|---|---|
| **Saldırı Yap** | $-92, -168$ | $194, -224$ |
| **Saldırma** | $0, -180$ | 0,0 |

Tablo 9 - SoY VT Sunucusu Çözüm Matrisi

Saldırganın ve savunanın karakteristik fonksiyonları hesaplandıktan sonra ortaya çıkan sonuç matrisleri Tablo 9 ve Tablo 10'da gösterilmiştir.

Nash dengesine göre, her sonlu oyunda en az bir denge noktası bulunmaktadır. Tablo 10'da 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.

| | Savun | Önlem Alma |
|---|---|---|
| **Saldırı Yap** | $-100, -160$ | $110, -140$ |
| **Saldırma** | $0, -180$ | 0,0 |

Tablo 10 - SoA VT Sunucusu Çözüm Matrisi

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 saldırsa da saldırmasa da aynı bedeli almaktadır. Aynı şekilde saldırgan 0,79 olasılıkla saldırı gerçekleştirir ise, savunanın güvenlik önlemi alması ve alamaması 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 ölçeklendirebilir güvenlik sağlanmaktadır. Bütün sistem üzerinde uygulanacak ve uzun sürecek ve güvenlik değerlendirme yöntemi kısaltılmakta ve dinamikleştirilmektedir.

## V. Sonuç ve Öneriler

Günümüz yöntemleri bulut bilişimde saldırgan ve savunanın kazançlarını ve masraflarını ön plana çıkarmamaktadır. Bu çalışma, bulut bilişim kullanılması durumda ideal güvenlik önlemlerinin bulunmasında yardım etmektedir. Önerilen modelde ekonomide çok sık kullanılan oyun teorisini kullanarak 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 yapacağı farklı tipteki saldırıları çözüm matrisinde farklı satırlara konarak ve buna karşı savunanın uygulayabileceği güvenlik önlemler de farklı sütunlara konarak çözüm matrisi büyütülmesi gelecekte yapılacak çalışmalar arasındadır. Bu şekilde ortaya çıkan matriste, saldırganın saldırılarından cayması için savunanın hangi güvenlik önlemini 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 Timothy Grance, "The NIST definition of cloud computing" National Institute of Standards and Technology Special Publication 800-145, Sept. 2011

[2] S. and Eloff, M.M. and Smith, E. Ramgovind, "The management of security in Cloud computing," Information Security for South Africa (ISSA), 2010, vol. 1-7, 2010.

[3] LIU Peiyu, LIU Dong, The New Risk Assessment Model for Information System in Cloud Computing Environment, Procedia Engineering, Volume 15, 2011, Pages 3200-3204, ISSN 1877-7058,

[4] Sajjan Shiva, Sankardas Roy, and Dipankar Dasgupta. 2010. Game theory for cyber security. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10), Frederick T. Sheldon, Stacy Prowell, Robert K. Abercrombie, and Axel Krings (Eds.). ACM, New York, NY, USA, , Article 34 , 4 pages

[5] James A. Kupsch, Barton P. Miller, Elisa Heymann, and Eduardo César. 2010. First principles vulnerability assessment. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW '10). ACM, New York, NY, USA, 87-92

[6] European Network and information Security Agency, "Cloud Computing Security Risk Assessment".

[7] P.G. Dorey, A. Leite, Commentary : Cloud computing – A security problem or solution?, Information Security Technical Report, Volume 16, Issues 3–4, August–November 2011, Pages 89-96, ISSN 1363-4127

[8] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing 3.0".

[9] Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and MateiZaharia Michael Armbrust, "Above the Clouds: A Berkeley View of Cloud Computing," Commun. ACM 53, 4 , pp. 50-80, April 2010.

[10] Nisan N, Roughgarden T, Tardos E, Vazirani V, editors. Algorithmic game theory. Cambridge University Press, 2007

[11] Dan Svantesson, Roger Clarke, Privacy and consumer risks in cloud computing, Computer Law & Security Review, Volume 26, Issue 4, July 2010, Pages 391-397, ISSN 0267-3649

[12] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0116

[13] DimitriosZissis, DimitriosLekkas, Addressing cloud computing security issues, Future Generation Computer Systems, Volume 28, Issue 3, March 2012, Pages 583-592, ISSN 0167-739X

[14] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," *IEEE Trans. Neural Networks*, vol. 4, pp. 570–578, Jul. 1993.