Protection of Security and Privacy on Cloud Computing: Dimension of Computational Defense and Legal Framework

Data · January 2014

CITATIONS
0

READS
874

1 author:

Ahmet Fatih Kılıç
Aydın Adnan Menderes University
2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

BULUT BİLİŞİMDE GİZLİLİK VE GÜVENLİĞİN KORUNMASI: BİLİŞİMSEL SAVUNMA VE HUKUKİ ÇERÇEVE BOYUTLARI

Ahmet Fatih Kılıç

Sakarya Üniversitesi, SBE, Yön. Bil. Sis., Y. Lis. Prog., ahmet.kilic@ogr.sakarya.edu.tr

Özet

Bulut bilişimin günümüzde sağlayacağı kolaylıklar ve getirmiş olduğu yeniliklerin yanında, veri odaklı bir tehlikeye de maruz kalması kaçınılmaz olabilir. Yapılabilecek herhangi bir olası saldırı durumunda bulut bilişimin ne şekilde korunacağına dair yapılan çalışmalarda birtakım önergeler yer almaktadır ve hukuk boyutuyla da temeli oluşturabilecek standartlar belirli kısıtlar içerisinde meydana gelmiştir. Ancak yapılan çalışmalar kendi iç disiplinlerinde incelenmiş, bulut bilişimin korunması ve savunmasında karşılıklı bir etkileşim yer almamıştır. Bu noktadan yola çıkarak, bu çalışmada bulut bilişimin güvenlik ve gizlilik savunmasında iki esasa dayanmış bir şekilde korumanın sağlanması ve buna yönelik olarak da bu etkileşim içerisinde yer alan oyuncuların aralarındaki ilişkinin ne şekilde olması gerektiği basit bir model üzerinden gösterilmiştir.

Anahtar Sözcükler: Bulut Bilişim Güvenliği, Adli Bilişim

1. GİRİŞ

Son zamanlarda ülkemizde de yaygınlaşmaya başlayan bulut bilişim sistemleri, sağladıkları birçok yenilik ve faydalarının yanı sıra, bazı tehlikeleri ve zorlukları da beraberinde getirmektedir. Veri edinme, depolama, kullanma, paylaşım veya dağıtımı gibi içsel mekanizmalarda yer alan yazılım ve donanımsal sorunların yanında siber saldırılar, sızma, bilgi çalma, bilişim virüsü ve mantık bombası gibi birtakım veri güvenlik ve gizliliğini zarara uğratacak faktörler ön plana çıkmaktadır (Mahmutoğlu, 2013). Bu faktörler genel anlamda bilişim sistemlerini zarara uğratmasının yanı sıra bulut bilişimde de veri yolları, internet tabanlı veri depolama, ağ protokolleri gibi bulut sistemleri oluşturan temel öğelerini de etkileme hususunda bu saydığımız faktörler içerisine göstermemiz uygun olacaktır. Yapılan saldırılara karşı her ne kadar kurum ve kuruluşlarda yer alan bilişim sistemlerinin tam koruma sağladıkları büyük oranda kabul edilse de, bu durumun bulut bilişim güvenliği noktasında söylenmesi mümkün olmayacaktır. Çünkü, savunma sistemleri ve bu sistemlerin kimler tarafından sağlanacağı net bir şekilde belirlenmemiş olup bulut bilişim sistemlerini kullanan kurumların ülkemiz açısından korunabileceği herhangi bir yönetmelik veya kanun yürürlükte yer almamaktadır. Ayrıca veri erişim ihlalleri ve uygulamalardan kaynaklanan hukuki problemlerin ve yasal belirsizliklerin, hizmeti sağlayan kesimden hizmeti alan kesime doğru güvenlik boyutuyla henüz tam

manasıyla anlaşılabilmiş olmaması bulut bilişimin zafiyetini göstermektedir (Subashini ve Kavitha, 2011).

Son yıllarda yapılan araştırmalar neticesinde, görüyoruz ki, bulut bilişimle ilgili yaşanan problemlere ilişkin bir takım çözüm önerileri sunulmuş, sorunların çeşitli olabileceği gibi, bu sorunların giderilmesinde gerek modellemeler yoluyla gerekse teorik yapıyla uygulanabilecek birtakım çözümlerin de varlığı ortaya çıkmıştır. Ancak yapılan çalışmalar bulut bilişimin güvenliğini, gizliliğini ve sürdürebilirliğini sağlamak adına tek taraflı çalışmalar olup, hukuki boyutu ayrı bir konu başlığı olarak kaleme alınmıştır. Bu çalışmanın amacı olarak bu iki farklı boyutu bir araya getirerek hukuki boyutuyla yasalar, ahlak kuralları ve caydırıcılık özelliklerinin yanı sıra, teknolojik olarak bulut bilişimin savunulmasında saldırı tespiti, erişim engelleme ve kriptolama mantığı üzerinde durulmaya çalışılacaktır. Bunun için de yapacağımız çalışma bulut bilişime konu olan kişiler veya oyuncular arasındaki ilişkiyi inceleyerek ve veri edinimini kademeli olarak gerçekleştirip, mevcut koruma sistemlerini gerek hukuki boyutuyla, gerekse teknolojik boyutuyla hedef kitlenin yardımıyla etkinliğini ölçerek, yapılmak istenmektedir.

2. BULUT BİLİŞİM VE ÖZELLİKLERİ

Bulut bilişim; bir kuruluşun kendi bünyesinde ya da kamusal ağda, çok sayıda bilgisayar ve ağ cihazının birbirine bağlanması ile oluşturulan bir veri merkezi üzerine kurulu sanallaştırılmış bir ortamda, altyapı ve uygulamaların hizmet olarak sunulduğu dağıtım ve destek modelidir (Sevli ve Küçüksille, 2013). Bu modelde öne çıkan özellik sanallaştırma olarak karşımıza çıkmaktadır. Sanallaştırma, IBM firmasının ilk defa 1960lı yıllarda ortaya attığı ve "zaman paylaşımı" olarak tanıttığı bir teknolojidir. Sanallaştırma teknolojisi, birçok yapılar içerisinde yer alan, geleneksel bilişim sistemleri ortamında kurulmuştur. İşletim sistemlerinin sanallaştırılması aynı zamanda server sanallaştırılması olarak da isimlendirilmekte ve "bilgisayar fonksiyonlarını fiziksel olmayan veya sanallaştırılmış iki veya daha fazla bilgisayarmış gibi oluşturmanın yolu" olarak tanılanmıştır. Sanallaştırmada, kaynaklar çoklu ortamlara ayrılabilir veya paylaştırılabilir. Bu ortamlar sanal makineler (VMs) olarak bilinmektedir (Mishra ve diğerleri, 2013).

Sanallaştırma, Velte ve diğerlerine göre iki kısımdan ibarettir:

- Tam Sanallaştırma: Bu çeşit sanallaştırma diğer bir makine üzerinde çalışan kurulumu tamamlanmış sanallaştırmadır.

- Paravirtualization: Sistem kaynaklarını etkin bir şekilde kullanarak aynı anda sadece bir tane donanım aygıtını çalıştırmaya olanak sağlayan sanallaştırma şeklidir. Bu teknikle sanallaştırılan sistemler normal (tam) sanallaştırılmışlara göre çok daha hızlı çalışırlar. Ancak cpu desteği yoksa konuk işletim sisteminin de paravirtualization amaçlı modifiye edilmiş olması gerekir.

Bulut bilişimin kısımlarını şu şekilde sıralayabiliriz:

- Servis olarak altyapı
- Servis olarak platform
- Servis olarak yazılım

2.1. Servis Olarak Altyapı

Bulut bilişim altyapısındaki yığının en alt tabakasındaki fiziksel servisleri ifade eder. Bu tabaka; sanal makineler, yük dengeleme servisleri, ağa bağlı depolama servisleri gibi temel donanım servislerini içerir.

2.2. Servis Olarak Platform

Uygulama geliştirmek için kullanılan altyapıyı oluşturur. Bulut hizmeti alan kullanıcılar, geliştirdikleri uygulamaları, servis sağlayıcı tarafından sunulan platform üzerinde, özelleştirilmiş bir ortamda çalıştırırlar. Bu ortam çoğu zaman kısıtlanmış, düşük imtiyazlı bir yapıdadır.

2.3. Servis Olarak Yazılım

Hazırlanan bulut uygulamalarının sergilendiği katmanı ifade eder. Bir bulut altyapısı üzerinde çalışan uygulamalar, servis kullanıcılarına, bu katmanda hizmet olarak sunulmaktadır. Sunulan uygulamalara, internet üzerinden zaman ve konum kısıtlaması olmaksızın erişilebilmektedir (Sevli ve Küçüksille, 2013).

Genel itibariyle bulut bilişimin servisler açısından sırlaması literatürde bu şekilde yer almaktadır. mimari açıdan incelendiğinde ise özel bulut (kurumsal), genel bulut (kamusal), ve hibrit olarak adlandırılan kuruluşun kendi bünyesinde barındırıp yönettiği kaynaklarla, harici altyapı kaynaklarının birleştirilmesi sonucu oluşan bulut modelidir.

Diğer bir bulut bilişim gruplaması Mishra ve diğerlerinin çalışmalarında yer alan; uygulama seviyesi, orta seviye, işletim seviyesi ve donanım seviyesi olarak dört gruba ayrılmaktadır. Bu sırlamalar gerek problemlerin çözümünde gerekse etkinlik modeli oluşturmada katkı sağlayacak sınıflandırmalar yer almaktadır. Her bir gruplama, sistemin hitap ettiği kesimce farklı algılanmakta, bu şekilde bulut bilişimin yönetimini sağlayabilmektedir.

3. BULUT BİLİŞİM VE BİLİŞİMSEL SAVUNMA

Bulut bilişimin sistem boyutuyla korunmasına yönelik uygulama literatürüne katkı sağlayan metot ve modeller vardır. Bu modeller bulut bilişimin korunmasında gerek adli boyutuna katkı sağlamak, gerekse sistem kısmında savunmayı sağlamak amaçlı çeşitli uygulamalardan oluşmaktadır. Rongxing ve diğerlerinin yapmış oldukları çalışmada, bulut bilişime uyarlamak istedikleri güvenlik özellikleri sayesinde adli veriler üretebilecek matematiksel tabanlı bir tasarımdan bahsedilmektedir. İkili eşleştirme metodu ismini verdikleri bu model, kurulum, K-Gen, anonim-yetki, yetki-erişim ve takibatı sağlama olarak beş kısımdan oluşmuştur. Bu modelin dezavantajı anlaşılması zor ve kompleks matematiksel formüllerle tasarlanmış olmasıdır(2010). Buna karşın Jansen'in yapmış olduğu teorik çalışmada bulut bilişim ile ilgili güvenlik sorunlarını kullanıcılara öğretmek yönünde bir çalışma yer almış, kurumsal olarak bulut bilişimin veri güvenliğini karar verme safhalarında ele alarak gerekli olan güvenin sağlanmasını kapsam içerisine almıştır(2011). Jansen'in yapmış olduğu bu çalışmaya benzer olarak Sumter'in güvenilir bulut bilişim platformu metodunun, bulut bilişim kullanıcılarına güvenlik riskini azaltma ve güvence sağlama hususlarında etkili olduğu iddia edilmektedir. Sumter, yapmış olduğu modeli küçük ölçekli bulut ortamında vaka çalışması olarak test etmiş, yetkisiz erişimleri

engellemek için veri hareketlerini yakalayan ve proses süreçlerinde bu işlemlerin bulut sistemi üzerinde yer almasını sağlayan bir sistem tasarımını kullanmıştır (2010).

Bleikertz ve diğerlerine göre bulut bilişim ile ilgili güvenlik ve gizlilik sorunlarının bulut bilişimin sağlayacağı faydayı gölgeleyeceğini ifade etmişlerdir. Bulut bilişimin görünürde oldukça esnek bir yapıya sahip olmalarına rağmen kendi içerisinde karmaşıklık barındırdığı ve web ara yüzleri kullanılarak konfigüre edildiği bir sistem olduğunu söylemişlerdir. Bu öngörülerden yola çıkarak Amazon.com'un Elastik Bulut (EC2) adı verdikleri sistemi değerlendirmeye almışlardır. Öncelikle erişebilirlik ve güvenlik açıklarına odaklanılmış güvenli analiz modeli uygulanmış ve gerçekçi ortamlar için etkinlik ölçümü yapılmıştır. Çalışmanın sonucunda kendi iddialarına göre karmaşık bulut altyapılarının konfigürasyonlarını doğrulayarak mevcut güvenlik sorunlarını etkin bir şekilde düzeltebileceklerini vurgulamışlardır (2010).

Lombardi ve Di Pietro, yaptıkları çalışmada şeffaflık üzerinde durmuşlar ve bulut içerisinde bütünlüğün sağlanması için Şeffaf Bulut Koruma Sistemi (TCPS) adlı güvenlik mimarisini öne sürmüşlerdir(2010). Şeffaflık konusu veri paylaşım ve güvenliği noktasında üzerinde durulması gereklidir. Güvenli bir şekilde verilerin kamuoyu ve diğer veri ihtiyacı olan kesimlerle paylaşımında şeffaflık yasallık taşıması adına önemli bir faktördür.

Bulut bilişimin güvenliğini ele aldığımızda, dışsal bir platform kullanması neticesinde saldırılara açık bir konumda olduğunu görürüz. Ağ yapıları üzerinden sağlanan bu hizmetin saldırılara açık olması, verilerin nasıl korunması gerektiğini aklımıza getirebilir. Bu konumda verilerin sınıflandırılması, hassas ve diğer veriler olarak iki kategoriye ayrılması faydalı olduğu düşünülmektedir (Henkoğlu ve Külcü, 2013). Bu sayede verilerin ayrıştırılması, gizlenmesi ve güvenliğinin sağlanması, dış tehditlere karşı alınabilecek önlemlerin başında geldiği söylenebilir. Hasssas verileri kriptolamak ve diğer verileri standart bir şekilde depolamak hem etkinlik hem de maliyetleri kontrol etme açısından önem kazanacaktır.

Güvenli Bulut Bilişim

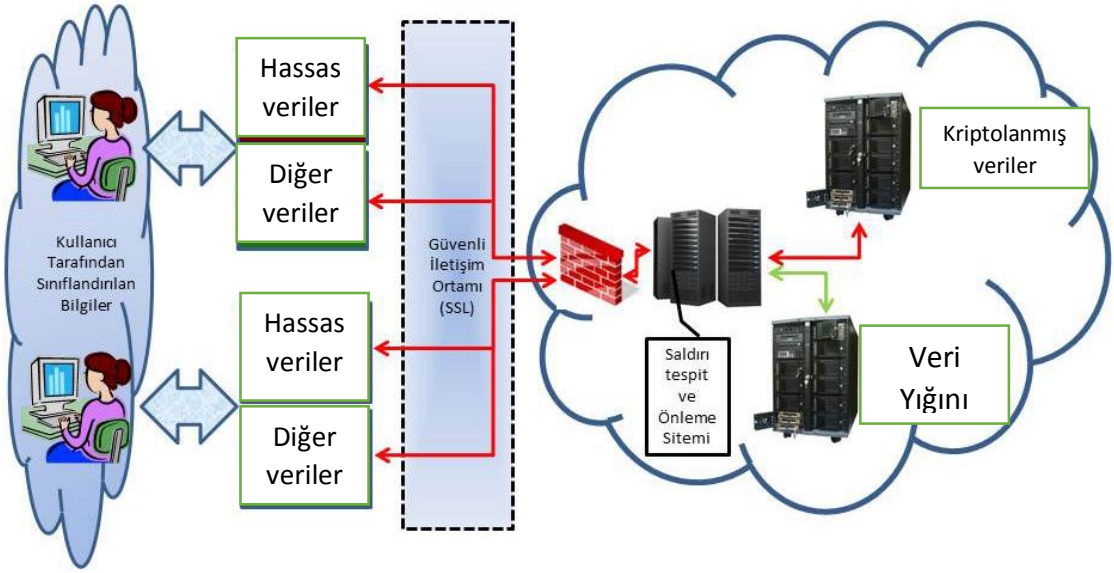
Bulut bilişim güvenliğini sağlaması adına ülkemizde geliştirilmiş herhangi bir standart yer almamıştır. Bulut güvenliğinin sağlanması genelde verilerin korunması noktasında karşımıza çıkmaktadır. Yapılan çalışmalarda bankacılık sektöründe veri güvenliğini sağlamak amacıyla düzenlenen 5411 Sayılı Bankacılık Kanununun bilişim sistemleri üzerinde veri güvenliğini sağlamak için başvurulabilecek bir kaynak olduğu öne sürülmektedir (Henkoğlu ve Külcü, 2013). Bu kanunun veri güvenliği açısından uygulanabilmesi neticesinde güvenli bulut bilişim modelini aktif hale gelip, kullanıcıya açılmasına imkan vereceği söylenmektedir.

Bulut bilişimde güvenliği sağlamak birtakım gereksinimleri ön plana çıkarmaktadır. Genel anlamıyla güvenli bir bulut bilişim sağlanması aşağıdaki koşulların gerçekleştirilmesiyle meydana gelmektedir (Svantesson ve Clarke, 2010):

- Bulut servisi telekomünikasyon ağları üzerinden sağlanan bir hizmet olması;
- Kullanıcıların, veri erişimlerinde ve veri girişlerinde güvenilebilen bir servis sağlaması;
- Verilerin kullanıcılar tarafından uygun prosedürler içerisinde kontrol edilmesi;

- Kullanıcıların, teknik farkındalığı gerektirmeyen, hangi hizmet sağlayıcı tarafından servisin yapıldığını veya sanal makinelerin nerede olduğunun bilinmesine ihtiyaç duyulmaksızın kaynakların sanallaştırılmış olması;
- Hizmet sözleşmesinin nispeten de olsa esnek bir yapı içerisinde hazırlanması.

Bu prosedürlerden yola çıkarak verileri Tablo 1'deki gibi sınıflandırmaya tabi tutup bulut bilişim güvenliğini bir ölçüde sağlama olanağı vardır.



Tablo 1: Güvenli Bulut Bilişim Modeli **Kaynak:** Henkoğlu ve Külcü, 2013

Bulut bilişimle ilgili teknolojik savunma ve güvenlik tedbirlerini genel çerçeve içerisinde değinilmiş oldu. Hukuki boyutuyla bulut bilişimde caydırma, kanunlar ve belirli standartlar içerisinde koruma tedbirlerine bundan sonraki kısımda değinmeye çalışacağız.

4. BULUT BİLİŞİMİN HUKUKİ BOYUTU

Bulutta yer alan verilerin korunması normal veri depolama sistemlerinde ve yazılımlarda uygulanan prosedürler gibi olması beklenemez. Adli vaka olarak, delil toplama işlemleri, olay yeri inceleme, kriminal çalışmaların yapılması zordur. Sistemin ağ yapıları üzerinden hizmet vermesi, sanallaştırma ile birlikte depolanan verilerin ve depolama birimlerinin lokasyonunun bilinmemesi, bilinse bile zilyetliğin, mülkiyetin korunmasına zarar verecek yönde bir inceleme başlatılması, bilişimde adli delil toplama yönünden uygulamayı zorlaştıracaktır. Buna bağlı olarak ülkemizde, bilişim hukuku ve adli bilişim üzerinde yapılan çalışmalar henüz yeni yeni şekillenmeye başlamışken, bulut bilişim ile ilgili kısımlarda bu konu ile ilgili ibareler yer almamaktadır. Ancak, şu kadar var ki, veri güvenliği ve gizliliğini korumaya yönelik hükümler, sadece bulut ile ilgili olmayıp genel bir mecrada uygulama alanı bulmuşlarsa da, bulut bilişimde de yer edinebilecek özellikleri vardır. Bulut adli bilişim, bulut bilişim ile dijital adli bilişimin bir alt kesişim noktasında, ağ adli bilişimin bir alt kısmını teşkil etmektedir. Ağ adli bilişim, bilgisayar ağları üzerinde yapılan adli soruşturmalar ile ilgilidir. Bulut bilişimin de geniş bir ağ üzerinde kurulu olmasından dolayı bulut adli bilişim, ağ adli bilişimin temel süreçlerini esas alır (Ruan ve Diğerleri, 2011, akt: Sevli ve Küçüksille, 2013).

Bulut bilişimde uygulanacak hukuk kurallarını belirlemek, ülkeler arasında bir sorunu da gündeme getirmektedir. Şayet bulut hizmeti veren kuruluşlar ile hizmet alıcıların tabi olduğu kuralların belirlenmesi, hangi ülkenin hukuk kurallarına bağlı kalınacağı uluslararası düzeyde bir problem olarak karşımıza çıkmaktadır. Bundan öte bu depolama ve işletim sürecinde saklanılacak olan verilerin bulunduğu yerde böyle bir kuralın bulunmaması durumunda mağduriyetin artacağı da bir gerçektir. Bunların yanı sıra geleneksel bilişim sistemlerinin bu tür uygulamaları, bulut bilişime uyarlanması uyuşmazlığı da beraberinde getirebilmektedir (Taylor ve Diğerleri, 2010). Uyuşmazlıklar yalnızca bulut bilişimin korunması hususunda değil, ülkelerin kendi hükümlerinde yer alan kısımlarda da karşımıza çıkabilmektedir (Gray, 2013).

Tüm bu görüşlerin yanı sıra uluslararası açık bir sistem olması münasebetiyle bulut bilişime uyarlanabilecek kurallar sınırlıdır. Bu konu ile ilgili muhtelif görüşlere yer verilmiştir. Üzerinde 15 yıldır değişiklik yapılan "Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı" bulut bilişim de verilerin korunmasına yönelik referans alınabilecek kaynaklardan biridir(Henkoğlu ve Külcü, 2013). Ancak henüz yasalaşmamış olması ve bilişimin hızlı değişim sürecine ayak uydurabilme kabiliyeti de tartışma konusudur.

Bir diğer görüşe göre uygulanabilecek bir hukuk kuralı olarak "Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun" bir diğer referans noktasıdır. Bu kanunda yer alan hükümler 24.madde üzerinden düzenlenmiş olup, kamu düzenine aykırı olmayacak bir şekilde hizmet sağlayanlar ve hizmet alıcıları arasında her türlü anlaşmanın yapılabileceğine imkan vermiştir (Başgül ve Chouseinoglou, 2013). Ancak bu kanun belli başlı anlaşmazlıkları gidermekte yetersiz kalmakta, sözleşmenin tarafları arasında çıkabilecek herhangi bir uyuşmazlıkta hakem taraf olmayı benimsememektedir.

Gerekli Veri Kullanım ve Paylaşım Ölçütü

Verilerin kullanılması ve yasal yollardan elde edilmesine yönelik çalışmaların henüz kalıplaşmış şekliyle kullanılması ülkemiz açısından uygulanabilecek durumda değil. Ancak verilerin paylaşılması ve kullandırılması noktasında elbette özel hukuk alanında açık kapı bırakılmıştır. Ne var ki, bugün ülkemizdeki orta ve büyük çaplı firmalar bu boşluğun neticesi olarak bilgilerini paylaşmaktan imtina etmektedir.

Bu konu ile ilgili olarak belirli çözüm önerileri sunulmuş, bazı modeller ile çözüm önerileri yapılmıştır. Veri güvenliğine zarar vermeden uygun bir şekilde paylaşımın yapılmasına yönelik geniş kapsamlı model olarak Tablo 2'deki örneği gösterebiliriz. Güvenli koruma ile adli bilgi uygulama esasları (FIPPs)[1] arasındaki ilişkiyi gösteren bu model ile bilgi paylaşımları etkin, güvenilir ve düzenli bir şekilde paylaşıma açılabileceği savunulmaktadır.

Buradaki gizlilik anlamı hukuken yetkili kişiler tarafından ifşa edilebilmesi ve uygun kimseler tarafından kullanılabilmesi olarak tanımlanmıştır. Ancak kullanım sürecinde verilerin yanlış olması veya yanlışlıkla değiştirilmesine yönelik bilgi ve bilişim sistemlerinin korunması kısaca bütünlüğün sağlanması da önemlidir. Bunun ötesinde kullanılabilirlikte önemli olan yetkili kişiler tarafından vakitli ve güvenilir bir şekilde

[1] FIPPs: Fair Information Practice Principles, "Adli Bilgi Uygulama Esasları" olarak çevrilmiştir.

bilginin ve bilişim sistemlerinin kullanılmasına verdikleri güvence de ön plana çıkabilmektedir (Fedeal Chief Information Officers Council, 2011).

Bu şekil, yetkisiz girişler, kullanım, ortaya çıkarma, değiştirme, tahrip etme gibi faaliyetleri önlemek için gerekli olan bulut bilişim uygulamalarını belirtmek amaçlı gizlilik (FIPPs) ve güvenli koruma arasındaki ilişkiyi göstermektedir.

Tablo 2: Güvenli Koruma İle Adli Bilgi Uygulama Esasları (FIPPs) Arasındaki İlişki
Kaynak: Joint Task Force Transformation Initiative Interagency Working Group, 2012

FIPPs uluslararası kabul görmüş bir çerçeve sağlar ve ABD'nin gizlilik gereksinim yasalarına yansıtılmaktadır. Aynı zamanda bu model gizlilik riskini analiz etmek ve uygun hafifletme stratejisini benimsemek için hizmet sağlar (Joint Task Force Transformation Initiative Interagency Working Group, 2012).

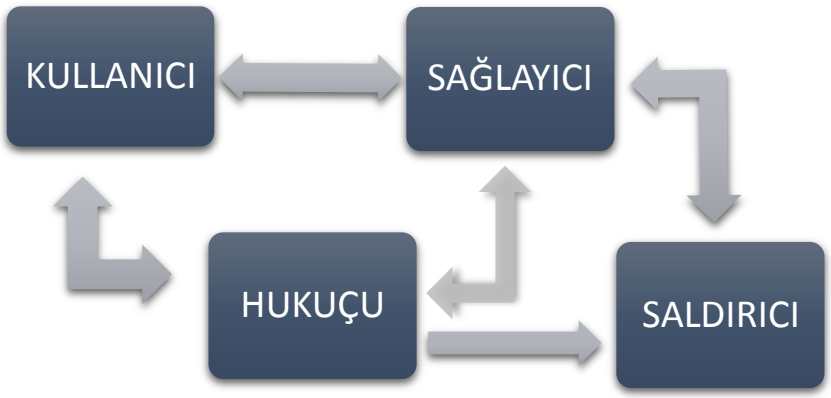
Bu modelin içsel korumasının yanı sıra dışsal olarak yönetimsel, teknik ve fiziksel korumalar da bu standart uygulamaları kapsayarak tamamlayıcı bir yapıyı oluşturmaktadır. Uluslararası uygulanabilir bir çerçeve sunması neticesinde ülkemizde veri güvenliğini ve gerekli paylaşımları sağlamak için referans olarak gösterilebilecek kapsamlı bir modeldir. Bu sayede analistlerin ve diğer veri ihtiyacı duyan kişi, kurum veya kuruluşların bu ihtiyaçlarını karşılayacak gerekli prosedürleri ve güvenliği yerine getirebilecek bir model olarak da ele alınabilir.

5. BULUT BİLİŞİMDE OYUNCU-ROL İLİŞKİ MODELİ

Bu kısımda, bulut bilişimin güvenliğinde etkin rol oynayan, gerek bireysel gerekse kuruluş bazında etkinliği sağlayan oyuncular ve aralarındaki ilişkiler ele alınmaktadır. Bu sayede, hem bilişim yönünden hem de hukuk açısından bulut bilişim, veri güvenliği, erişim kontrolü, saldırılar, korunma yöntemleri, caydırıcılık, savunma sistemlerini güçlendirme veya geliştirme yönünden fayda sağlayacağı beklenmektedir.

Bu model, esas alınan oyuncular ve ilişkiler "Bulut bilişim güvenliği ne kadar etkin, daha iyiye nasıl ulaşabiliriz?" sorularına cevap arama niteliğinde, sürekli gelişim yolunu izlemek için tasarlanmıştır. Genel olarak diğer çalışmalarda, bilişim sistemlerinin yazılımsal ve donanımsal yönü, hukuk açısından kanunlar, hükümler, uygulama alanları esas alınmışken, bu modelde esas aldığımız uygulayıcılar, hizmet sunanlar, hizmet alıcıları, saldırıcılar ve hukuk kesimidir.

Literatüre katkı sağlamak ve yeni çalışmalara fikir vermek adına uygulanmak istenen bu model Tablo 3'te basit bir ilişkisel model üzerinden gösterilmiştir.



Tablo 3: Bulut Bilişimde Rol Alan Oyuncuların İlişkisel Modeli

Modelde yer alan faktörler iki taralı incelenmektedir. Birincisi kendi içlerinde sahip oldukları özellikleri, yapıları ve görevleriyle, ikincisi ise bunlar arasındaki ilişkileri ele alınarak tanımlanmaktadır.

5.1. Model Oyuncuları

Değinildiği üzere oyuncuların kendi yapıları, özellikleri ve görevleriyle incelemeye konu olmaktadır.

5.1.1. Kullanıcılar

Esas hizmeti alan kişiler veya kurumlar olarak tanımlayabiliriz. Alınan hizmetin kalitesini, işlevselliğini artırmada, görünmeyen kısımların açığa çıkarmada etkilidirler. Servis alıcıları, bulut hizmeti kullanımında sistemi geliştirme adına ihtiyaçlarını dile getirip, sistemlerin ne şekilde tasarlanması gerektiğine dair hizmeti sunan taraflara fikir verebilirler. Güvenlik sorunlarından önemli ölçüde etkilenecek kısımda yer alırlar.

5.1.2. Hizmet Sağlayıcıları

Sistem geliştiricileri ve hizmet sunan kesim, hizmet verdikleri müşterilerine odaklanmalarının yanı sıra, diğer taraftan, bulut bilişimin saldırılara açık olması nedeniyle güvenlik problemleriyle de başa çıkmaya çalışmaktadırlar. Saldırılarla muhatap olacak ve saldırılara karşı savunmanın yapılacağı iki taraflı bir etkileşim içerisinde yer almaktadır.

5.1.3. Hukuk Kesimi

Adli bilişimde rol oynayan bu kısım, standartları belirleme, prosedürler oluşturma, arabuluculuk ve düzenleme konularında etkilidir. Bulut bilişimde güvenliğin sağlanması, caydırıcılık yönünden de kısmen mümkün olmaktadır. Ancak ülkemizde kabul edilebilecek bir oranda (%7) olmayıp, bu hususta çalışmaların artırılması gereklidir (ISC, 2012).

5.1.4. Saldırıcılar

Genel olarak "hacker" diye tabir ettiğimiz bu kısımda 8 tür karşımıza çıkmaktadır (Wikipedia, 2014):

Hacktivist: Hacktivist'ler kendilerine göre kötü veya yanlış olan toplumsal veya politik sorunları dile getirmek amacıyla belirli siteleri hack'leyerek mesajlarını yerleştirirler.

Siyah şapkalı: Her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabilen bu en bilindik hacker'lar, sistemleri kullanılmaz hale getirir veya gizli bilgileri çalar. En zararlı hacker'lar siyah şapkalılardır.

Beyaz şapkalı: Beyaz şapkalılar da her türlü programı, siteyi veya bilgisayarı güvenlik açıklarından yararlanarak kırabiliyor ancak kırdığı sistemin açıklarını sistem yöneticisine bildirerek, o açıkların kapatılması ve zararlı kişilerden korunmasını sağlıyorlar.

Gri şapkalı: Yasallık sınırında saldırı yapan, iyi veya kötü olabilen hacker'lardır.

Yazılım korsanı: Yazılım korsanları bilgisayar programlarının kopya korumalarını kırarak, bu programları izinsiz olarak dağıtımına olanak sağlayıp para kazanırlar. Piyasaya korsan oyun ve program CD'lerini yazılım korsanları sağlar.

Phreaker: Telefon ağları üzerinde çalışan, telefon sistemlerini hackleyerek bedava görüşme yapmaya çalışan kişilerdir.

Script Kiddie: Script kiddie'ler hacker'lığa özenen kişilerdir. Tam anlamıyla hacker değillerdir. Script kiddieler genellikle kişilerin e-posta veya anında mesajlaşma şifrelerini çalarlar.

Lamer: Ne yaptığının tam olarak farkında olmayan, bilgisayar korsanlığı yapabilmek için yeterince bilgisi olmayan kişi. Script Kiddie benzeri kişilerdir.

Hackerlar, her ne kadar kötü bir izlenim uyandırsalar bile, sistemi daha iyi hale getirmek için hizmet sunuculara ilham kaynağı olabilmektedir. Özellikle beyaz şapkalı hacker olarak tanımlanan kısım sistem geliştiricilere büyük ölçüde katkı sağlayabilmektedir. Güvenlik ve savunma etkinliğini ölçmede bu hackerlardan faydalanılabilir. Ancak elbette bu yasal sınırlar içerisinde veya hizmet sağlayıcıları ve geliştiricileri ile bu hackerlar arasında yapılacak olan bir sözleşme ile gerçekleştirilebilir.

5.2. Oyuncular Arası ilişkiler

Bulut bilişim güvenliğinde bahsettiğimiz oyuncuları dört kısma ayırmıştık. Bunlar arasındaki doğrudan veya dolaylı bir şekilde ortaya çıkan ilişkileri de ikili veya üçlü olarak yine dört kısma ayıracağız:

5.2.1. Temel İlişki Durumu (Kullanıcı-Sağlayıcı)

Bu ilişkide yer alan oyuncular, kendi görevlerinin yanı sıra birbirlerine karşı olan sorumluluklarını da bilmeleri gerekmektedir. Hizmet sağlayıcının verdiği hizmet kalitesi, güvenlik boyutu ve bunun gibi hizmet özelliklerini sağlamasının yanı sıra, hizmet alan kişilerin veya kuruluşların da aldıkları hizmeti uygun bir şekilde kullanarak geliştiricilere hem kendi menfaatleri için hem de sürekliliği sağlamak için yardımcı olmaları gerekir.

5.2.2. Olağan Durum (Kullanıcı-Sağlayıcı-Hukukçu)

Bu ilişki düzenleyici bir etki oluşturmak için gereklidir. Aynı zamanda ihtilaf noktalarında arabuluculuk hizmeti olarak da değerlendirilebilir. Örneğin bulut bilişimin güvenliği konusunda savunma stratejilerini hangi tarafın oluşturacağı, hizmet veren kesimin hangi hizmet standartlarını benimsemesi gerektiği, kullanıcıların hizmet alırken ne şekilde davranacağına yönelik yol gösterme hususlarında düzenleyici bir etkisinin olacağı beklenmektedir.

5.2.3. Elektronik Savaş Durumu (Sağlayıcılar-Kullanıcılar-Saldırıcılar)

Kötü niyet sahibi kişilerin olmaması durumunda sadece bulut bilişimde değil her bir bilişim alanında dışsal bir savunma mekanizmasına ihtiyaç olmayıp, sadece içsel güvenlik problemlerine odaklanılabilirdi. Ancak bu kişilerin varlığı her alanda güvenlik tedbirlerinin alınmasını gerekli kılmaktadır. Yapılan saldırıların ilk başta kullanıcıları etkilediği ve büyük kayıplara neden olduğu bilinmektedir. Bu saldırılara karşı alınacak önlemler, birincil dereceden ve büyük oranda hizmet sağlayıcı kesimden uygulanması nedeniyle muhatap olan kısım da sağlayıcılar olacaktır. Ancak yapılan saldırılara karşı bir tepki olarak hizmet sağlayıcıların da saldırıyla cevap vermesi uygun olmaz. Hizmet sağlayıcıların yapılan saldırı tekniklerine karşı yapacağı savunma teknikleri daha makul olacaktır. Aslında caydırıcılık etkisi hukuk kesiminden önce bu noktada ön plana çıkmaktadır.

5.2.4. Caydırma Etkisi (Hukukçu-Saldırıcı)

Hizmet sağlayıcıların saldırılara karşı yapmış olduğu savunmaların yetersiz kalması ve kullanıcıların da mağdur olması durumunda, hukuk boyutu kısmen de olsa baskısını göstermektedir. Bu durum olağan işleyişe farklı bir disiplinden destek olmaktadır. Hukuk kurallarının niteliği ve uygulanacak olan cezaların caydırıcılığı yönünden bu desteği sağlamaktadır. Olağan durumda olduğu gibi bu ilişkide de bir düzenleyicilik söz konusudur. Ancak ülkemizde bu başlığın altı uygun ve olması gibi doldurulmalıdır. Yani hukukun etkinliği bulut bilişim alanında kendisini göstermesi durumunda bu model büyük oranda işlevsel hale gelebilecektir.

Yukarda sağdığımız modelin ilişkileri güvenliğin sürekli olarak devam ettirilmesi açısından önemli olduğunu düşünüyoruz. Bu nedenle ilişkilerden yola çıkarak güvenliğin hem bilişim hem de hukuksal açıdan yerine getirilmesi adına çalışma yapmayı hedefliyoruz.

5.3. İlişkisel Modelde Veri Edinim Yolu

Kullanacağımız yöntem, mülakat ile saldırıcı olarak nitelendirdiğimiz gruptan bilgi sağlamak olacaktır. Ancak hizmet alanları, sağlayanları ve hukuk kesimini görmezden gelip bu şekilde bilgi toplamanın uygun olmayacağını düşünüyoruz. Bu nedenle başlangıç noktası olarak kullanıcıları hedef alıp tam olarak yapılandırılmamış bir şekilde anket veya mülakat uygulanmak istenmektedir. Daha sonra alınan cevaplar neticesinde güvenlikle ilgili kısımlar ön plana çıkarılıp yenileme yoluyla anket veya mülakatlar yeniden tasarlanacak, bu sefer sağlayıcılar grubuyla etkileşime geçip onların görüşleri alınacaktır. Hem kullanıcı hem de sağlayıcı örneklemlerinden almış olduğumuz bilgileri hukuki şekil içerisine koyarak hukuk kesiminin de fikirleri alınacaktır. En son bütün topladığımız bilgileri revize ederek saldırıcı gruplarıyla görüşülmesi istenmektedir.

Yapacağımız çalışmanın en zor kısmı hedef kitleden veri toplama olacaktır. Ancak güvenilir verilerin toplanmasının mümkün olmaması veya yeterli ölçüde uygun olmaması neticesinde olağan ilişki durumlarında topladığımız bilgiler güvenlik etkinliğinin ölçümünde bize gerekli olan bilgiyi sağlayacağını umuyoruz.

6. SONUÇ

Bulut bilişimin güvenlik problemlerine açık olması, sağlayacağı fayda yanında getireceği zorluklardan biridir. Ağ yapıları ve teknolojilerinin gelişmesine paralel olarak bulut bilişim, gelecekte firmaların maliyetlerini daha etkin bir şekilde kontrol altına alabileceği, önemli ölçüde tasarruf sağlayabileceği bir teknoloji olarak gösterilmektedir. Tüm bunların yanı sıra güvenlik teknolojilerini geliştirmede üzerinde durulacak bir alan da olabilir. Genellikle veri depolama işlemi için kullanılan ve firma ya da kuruluşların son zamanlarda rağbet etmeye başladığı bulut sistemlerin ne şekilde korunacağı tek taraflı çalışmalarda yer almış ikili bir karşılaştırma olarak bilişim ve hukuk eşleştirmesi literatürde rastlanmamıştır. Buna binaen bulut bilişimde ileriki çalışmalara destek olması adına ilişkisel bir model ortaya konmuştur. Bu model bulut bilişimde yer alan oyuncuları esas alarak aralarındaki ilişkiyi incelemiş, bu incelemeler neticesinde ilişkiler tanımlanmış ve daha iyi bir bulut bilişim güvenlik modelinin geliştirilmesinde ön ayak olması düşünülmüştür.

KAYNAKLAR

1. Prof. Dr. Fatih Selami MAHMUTOĞLU, **Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi**, İÜHFM C. LXXI, S. 1, s. 891-890, İstanbul, 2013

2. S. SUBASHİNİ, V. KAVITHA, **"A Survey on Security Issues in ServiceDelivery Models of Cloud Computing"**, Journal of Network and Computer Applications, vol.34 (1), pp.1-11, 2011.

3. Onur SEVLİ, Ecir Uğur KÜÇÜKSİLLE, **"Bulut Ortamında Adli Bilişim"**, 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Bildiriler Kitabı, Ankara, Eylül 2013

4. Ankur MISHRA, Ruchita MATHUR, Shishir JAIN, Jitendra Singh RATHORE,**"Cloud Computing Security"**, International Journal on Recent and Innovation Trends in Computing and Communication Volume: 1 Issue: 1, Rajasthan, India, 2013

5. RONGXING et al, **"Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing"**, ASIACCS 2010, Beijing, China.

6. Wayne A. JANSEN, **"Cloud Hooks: Security and Privacy Issues in Cloud Computing"**, 44th Hawaii International Conference on System Sciesnces, 2011.

7. R. La 'Quata SUMTER, **"Cloud Computing: Security Risk Classification"**, ACMSE 2010, Oxford, USA,.

8. Soren BLEIKERTZ et al, **"Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds"**, CCSW 2010, Chicago, USA.

9. Flavio LOMBARDI& Roberto Di PIETRO, **"Transparent Security for Cloud"** SAC March 22-26, 2010, Sierre, Switzerland.

10. Türkay HENKOĞLU ve Özgür KÜLCÜ, **"Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme"**, BİLGİ DÜNYASI, 2013, 14 (1) 62-86.

11. Dan SVANTESSON, Roger CLARKE, **"Privacy and consumer risks in cloud computing"**, Computer Law & Security Review, vol. 26, 2010, pp. 391-397.

12. K. RUAN, J. CARTY, T. KECHADİ, M. CROSBİE, **"Cloud Forensic"**, IFIP Advances in Information and Communication Technology, vol. 361, 2011, pp. 35-46.

13. M. Taylor, J. Haggerty, D. Gresty, R. Hegarty, **"Digital evidence in cloud computing systems"**, Computer Law & Security Review, vol. 26, 2010, pp. 304-308.

14. Anthony Gray, **"Conflict of laws and the cloud"**, Computer Law & Security Review, vol. 29, 2013, pp.59-65

15. M. Mürsel BAŞGÜL, Oumout CHOUSEINOGLOU, **"Bulut Bilişim Kapsamında Ortaya Çıkabilecek Hukuki Sorunlar"**, 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Bildiriler Kitabı, Ankara, Eylül 2013.

16. Federal Chief Information Officers Council, **"Federal enterprise architecture security and privacy profile (FEA-SPP)"**, version 3.0. Washington, DC: Office of Management and Budget; 2011.

17. Joint Task Force Transformation Initiative Interagency Working Group, **"Security and privacy controls for federal information system and organizations"**, NIST Special Publication (SP) 800–53 revision 4 (initial public draft),. Maryland: National Institute of Standards and Technology; 2012.

18. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı (ISCTURKEY 2012) Sonuç Bildirgesi, 2012.

19. Wikipedia, **"Hacker", http://tr.wikipedia.org/wiki/Hacker,** Erişim Tarihi: 02.01.2014