Bulut Ortamında Adli Bilişim

Onur SEVLİ, Ecir Uğur KÜÇÜKSİLLE

***Özet*—Bulut bilişim, sunduğu olanaklarla bilgi teknolojileri alanında önemli bir noktaya gelmiş ve son yıllarda bulut bilişime olan yönelim hızlı bir artış göstermiştir. Sunduğu imkânların yanında bir takım riskleri de beraberinde getiriyor olması bulut ortamına aktarılan verilerin güvenliği konusundaki kaygıları arttırmaktadır. Ayrıca bulut bilişim, yapısal özelliklerini çıkar amaçlı kullanmaya yönelen suçluların da hedefi haline gelmiştir. Bunun sonucu olarak bulut üzerinde işlenen bilişim suçları yaygınlaşmakta ve bulut üzerinde yapılan adli soruşturmaların önemi artmaktadır. Bulut üzerinden delil elde etme önemli hale gelmekte ve dijital adli bilişim bulut bilişimi de kapsayacak şekilde yeniden biçimlenmektedir.**

***Anahtar Kelimeler*—Adli bilişim, Bulut bilişim, Dijital delil, Veri güvenliği**

***Abstract* —Cloud computing has come to an important point in the field of information technologies thanks to the opportunities it provides. Recently, tendency to the cloud computing has remarkably grown. Besides it's opportunities cloud computing brings up a number of risks, thus security concerns for the data transferred to cloud environment have been increasing. In addition, cloud computing has become a target for criminals who tends to use cloud's structural features for their own benefits. As a result of these, cyber crimes on the cloud have been widespread and the importance of forensic investigations on the cloud has been increasing. Obtaining digital evidence from cloud environment has been becoming more important and digital forensics have been reshaping to cover the cloud computing.**

***Index Terms* —Computer forensic, Cloud computing, Digital evidence, Data security**

I. GİRİŞ

BİLGİ teknolojilerinin tarihi gelişim sürecinde, bir sistem ya da uygulama üzerinde depolanan verilerin, yasadışı erişimlere karşı hiçbir zaman, tam anlamıyla korunaklı olmadığı görülmektedir [1]. Bulut bilişim ortamlarında ise bu risk daha da artmaktadır.

Bulut bilişim, bir veri merkezindeki çok sayıda bilgisayarı birbirine bağlayıp bunlar üzerinde sanallaştırılmış bir platform oluşturarak, yazılım ve donanım servislerinin kullanımına yeni bir yaklaşım getiren dağıtım modelidir [2]–[3]. Kaynakların birden çok kullanıcı arasında paylaşımı temeline dayanan bulut bilişimde, kullanıcıların alt yapı yatırım maliyetleri sıfıra iner ve hizmet sağlayıcının sunduğu ortak altyapı kiralanarak kullanılır. Ancak bu ortak kullanım belirli güvenlik risklerini de beraberinde getirmektedir.

Bulut bilişim sistemleri, dijital verilerin dağıtık olarak işlenmesine yönelik yeni bir kavram ortaya koyar [4]. Veriler birden çok sunucu üzerinde, kullanıcıdan soyut bir şekilde, dağıtılarak işlenir. İşlem anında verilerin hangi konum ve cihazlar üzerinde yer aldığı konusunda hizmet kullanıcıları bilgi sahibi değildir. Bulut bilişim, bu dağıtık ve sanallaştırılmış yapısından dolayı kullanıcıların güvenlik kaygılarını arttırmaktadır [5]–[6].

Bulut servis sağlayıcıları, servis erişilebilirliği ve maliyet uygunluğunu sağlayabilmek için veri merkezlerini dünyanın farklı coğrafyalarına inşa ederler. Bir veri merkezinde depolanan veriler, güvenlik risklerini azaltmak için başka konumlara da yedeklenir [20]. Farklı ülkelerin veri güvenliği konusundaki farklı yaptırımları, adli bilişim soruşturmalarda sorun teşkil edebilmektedir [4].

Bulut bilişim, internet tabanlı bir model olmasından dolayı güvenlik tehditleri ve gizlilik ihlallerine açıktır [7]. Suçlular bulut bilişimi, suç delillerini saklamak, saldırılar yapmak, şifreleme anahtarlarını kırmak gibi çeşitli amaçlar için kullanmaktadırlar [8]. Bulut bilişim servisleri içerisinde en çok kullanılanlardan biri depolama servisidir [9]. Zaman içinde kuruluşlar, bulut depolama hizmetini kredi kartı bilgileri ve diğer hassas verilerini de depolamak amacıyla kullanmaya yönelmişlerdir. Suçlular bulut ortamındaki bu verileri hedef aldıkları zaman, karmaşık bir adli soruşturma süreci başlamakta ve dijital soruşturmacıların olayla ilgili delil elde edebilmeleri için zorlu bir yol izlemeleri gerekmektedir[8].

Adli bilişim, bilişim sistemleri üzerinden veri olarak elde edilen delillerin toplanması, saklanması, derlenmesi ve analizi konusunda ilke ve standartlar oluşturan disiplinler arası bir bilim dalıdır [10]. Bulut ortamlarında potansiyel dijital riskleri tanımlama, dijital delilleri elde etme ve analiz kritik bir öneme sahiptir. Geleneksel adli bilişim yaklaşımı bulut bilişime tam olarak hitap etmediğinden dolayı, adli bilişim süreci bulut bilişim üzerinde yeniden yapılanma yoluna gitmiştir.

II. BULUT BİLİŞİM

Bulut bilişim; bir kuruluşun kendi bünyesinde ya da kamusal bir 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. Bulut bilişim bilgisayarların yeteneklerini genişleterek, kullanıcıların bir veri merkezinde yer alan bir dizi yazılım ve

Onur SEVLİ, Mehmet Akif Ersoy Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, 1530, Burdur, Türkiye. (Telefon:+90 248 213 4130 e-mail: onursevli@mehmetakif.edu.tr).

Ecir Uğur KÜÇÜKSİLLE, Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 32260, Isparta, Türkiye. (e-mail: ecirkucuksille@sdu.edu.tr).

servise web servisi ya da web tarayıcı benzeri yazılımlarla, internet üzerinden erişebilmelerini sağlar [11] – [12].

Dijital cihazların ve internet kullanımının yaygınlaşması ile birlikte bulut bilişime rağbet artmıştır. Servis mimarisine dayalı bulut bilişim; veri ve uygulamalara, cihazdan bağımsız olarak erişebilmeyi, uygulamaların yaygınlaştırılıp kolaylıkla ölçeklenebilmesini sağlamaktadır. Bulut ortamına taşınan uygulamalar sayesinde yazılımlar pahalı birer ürün olmaktan çıkıp, "kullandığın kadar öde" mantığı ile hizmete sunulmuştur. Bu anlamda bulut bilişim uygulama geliştiriciler için de yeni bir pazar haline gelmiştir [13].

Zaman içinde bulut bilişim, teknolojik yaşamın vazgeçilmezi haline gelmiştir [14]. Bulut servislerinin kullanımı, büyük şirketlerin tekelinden çıkmış, küçük işletmeler ve bireysel kullanıcılar da bulutun işlem gücüne erişebilir hale gelmişlerdir.

A. *Bulut Bilişimin Karakteristik Özellikleri*

Bulut bilişimin temelinde aşağıdaki karakteristik özellikler yer almaktadır:

Sanallaştırma

Sanallaştırma; fiziksel bir kaynağı, ihtiyaçlar doğrultusunda, istenilen sayıda mantıksal parçaya bölerek, toplam sunucu verimliliğini optimize hale getirmeye yönelik bir teknolojidir. [15]. Bulut mimarisinde, bir veri merkezimin yekpare fiziksel altyapısı, sanallaştırma teknolojisi ile çok sayıda sanal sistem haline getirilip, her bir sistem farklı müşterilere hizmet olarak sunulabilmektedir.

İhtiyaca Bağlı Ölçekleme

Bulut bilişim platformları, kullanıcıların isteğine bağlı olarak, mevcut altyapıya yeni servis ve kaynakların eklenebilmesine imkân sunar. Yeni kaynak sisteme son derece hızlı bir şekilde eklenip, kullanıma hazır hale getirilir. Bu durum maliyet ve zaman açısından son derece kazançlıdır.

Farklı Coğrafyalarda Konuşlanmış Veri Merkezleri

Dünya çapında hizmet sunarken, farklı coğrafyalarda veri merkezlerine sahip olmak büyük öneme sahiptir. Bu yapının oluşturulması; ulusal ya da uluslararası yasalar, jeopolitik fikirler, yük dengeleme, ağ gecikmelerini minimuma indirme gibi durumlar açısından gereklidir [16].

B. *Bulut Bilişim Servisleri*

Kabul edilen üç genel bulut servis dağıtım modeli vardır:

Servis Olarak Altyapı (IaaS)

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

Şekil 1. Bulut bilişim servisleri

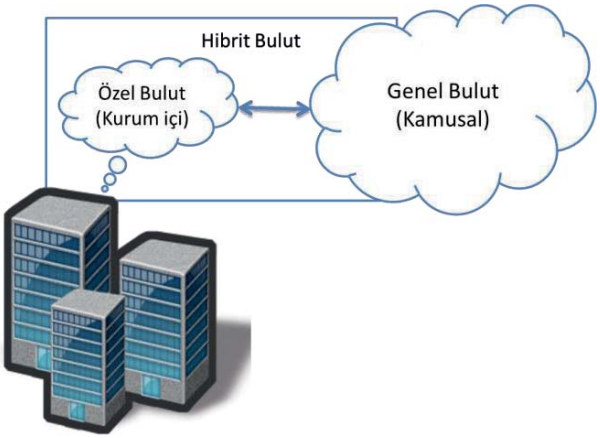
Servis Olarak Platform (PaaS)

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.

Servis Olarak Yazılım (SaaS)

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.

C. *Bulut Bilişim Mimari Modelleri*



Şekil 2. Bulut bilişim mimari modelleri

Özel Bulut

Bir kurumun kendi bünyesinde yer alan veri merkezleri üzerinde kurmuş olduğu bulut yapısıdır. Bilişim dünyasında uzun süredir uygulanan geleneksel modeldir. Veri güvenlik ve gizliliğinin üst düzeyde tutulmasını gerektiren durumlarda tercih edilmektedir. Özel bulut, bir güvenlik duvarının ardında, şirketin sınırlı sayıdaki kullanıcılarına hizmet vermektedir.

Genel Bulut

Standart olarak kabul edilen bulut bilişim modelidir. Bir

bulut servis sağlayıcı tarafından oluşturulan altyapı üzerindeki kaynaklar, uygulamalar, hizmetler, internet üzerinden kamusal ölçekte kullanıma sunulur. Veriler kamusal bir ağda yer alacağı için yapının kendine has güvenlik riskleri mevcuttur.

Hibrit Bulut

Bir kuruluşun kendi bünyesinde barındırıp yönettiği kaynaklarla, harici altyapı kaynaklarının birleştirilmesi sonucu oluşan bulut modelidir. Bu modelde kurum içi servislere harici bulut servisleri entegre edilip, bir bütün oluşturacak şekilde çalıştırılır.

D. Bulut Bilişimde Güvenlik ve Kriptografi

Güvenlik ve veri gizliliği, bulut bilişimin yaygınlaşması açısından önemli bir konudur [17]. Ancak bulut bilişimde aynı fiziksel altyapıyı birden fazla kullanıcının paylaşarak kullanması, altyapı üzerinde barındırılan verilerin güvenliği konusunda süregelen riskler oluşturmaktadır [18].

Bilhassa genel bulut mimarisinde kullanıcılar, hassas bilgilerin de içerisinde yer aldığı verilerini servis sağlayıcı altyapısında barındırma ihtiyacı duymaktadır. Bulut servis sağlayıcılar her ne kadar üst düzey güvenlik önlemleri alsalar da veri güvenliği konusundaki riskler bitmemektedir. Bulut mimarisinde farklı kullanıcıların ortak altyapıda depolama yapmalarından dolayı, bellek alanlarını birbirinden ayıran iç mekanizmalarda ortaya çıkabilecek sızıntılar yahut saldırılar sonucu kullanıcıların özel verilerinin üçüncü şahıslar tarafından ele geçirilme tehlikesi vardır [19].

Gizlilik ihlali riskinden korunmak için farklı yöntemler uygulanabilir. Bu yöntemlerden biri hibrit bulut modelini kullanıp gizliliği yüksek verileri kurum içi altyapılarda işlerken, güvenlik açısından risk teşkil etmeyen işlemleri genel bulut servisleri üzerinde gerçekleştirmektir.

Veri güvenliği ve gizliliği konusunda ortaya çıkan riskleri azaltmak için kullanılan bir başka temel yöntem ise kriptografidir. Homomorphic kriptografi gibi çeşitli algoritmalar ile şifrelenen veri, gizliliği ihlal eden üçüncü şahıslara karşı anlaşılmaz hale getirilmektedir. Kriptografik işlemler bulut servis sağlayıcılar tarafından gerçekleştirilebildiği gibi, veri sahibi kullanıcılar tarafından da yapılabilmektedir.

Kriptografi veri güvenliği için vazgeçilmez yöntemlerden biri olmakla birlikte, adli bilişim sürecinde belirli sorunlara yol açmaktadır. Bulut üzerinde elde edilen delillerin şifrelenmiş olması adli bilişim sürecine ek bir yük getirmektedir.

III. ADLİ BİLİŞİM

Teknolojinin gelişip yaygınlaşması ile birlikte bilişim suçları da artış göstermiştir. Bu durum suçla mücadelede, adli bilişimin önemini arttırmaktadır.

Adli bilişim; bilimsel prensipler ve teknolojik olanakların suçların çözümlenmesi ve yargılanmasında kullanılmasıdır. Diğer bir ifadeyle adli bilişim, bilgisayarlı soruşturma ve analiz tekniklerinin potansiyel delilleri tespit etmek amacıyla kullanılması olarak tanımlanabilir [21].

Geleneksel adli bilişim; bir soruşturmada ele geçirilen bilgisayar, yazılım, veri, işletim sistemlerinin analizi ile ilgilenmektedir. Fakat bu geleneksel bakış; kullanıcıdan uygulamalara, sunuculardan verilere kadar her yönüyle dağıtık olan bulut bilişim modelini tam anlamıyla kapsayamamaktadır.

A. Adli Bilişim Soruşturma Süreci

Adli bilişim soruşturmaları doğrusal bir işlem süreci izler. Bu sürecin temel adımları; tanımlama, çıkarım, analiz ve delilin sunumudur.

İlk aşamada, analist potansiyel delil kaynağını tanımlar: Şüphelenilen suç ne, şüpheli tarafından hangi donanım ya da yazılımlar kullanılmış, deliller nerede saklanıyor?

İkinci aşamada deliller, potansiyel kaynaklar üzerinden, bütünlüğü sağlanacak şekilde çıkarılır. Bilgisayar ortamı somut bir ortam değildir ve sanal ortamdaki veriler uçucudur. Analist bu uçuculuğun farkında olmalı ve çıkarım sürecinde bu problemi azaltacak araç ve teknikleri kullanmalıdır.

Üçüncü aşamada, çıkarım sonucu elde edilen veriler analiz edilir. Analiz, olay anında canlı olarak yapılabilir veya veriler bir adli bilişim laboratuvarına nakledilerek orada incelenebilir.

Son aşamada ise elde edilen sonuçlar, geçerli bir delil teşkil edecek şekilde hazır hale getirilir ve mahkemeye sunulur.

Bulut bilişim ortamında gerçekleştirilen adli bilişim süreci daha karmaşık yapıdadır. Bulutun dinamik ve dağıtık yapısından dolayı, altyapı üzerinden potansiyel delil verileri elde etmek ve verilerin doğruluğunu garanti edecek şekilde korumak daha zor bir hâl almaktadır.

IV. BULUT ORTAMINDA ADLİ BİLİŞİM

Bulut bilişimin sanallaştırılmış bir ortamda dağıtık veri işleme modeli, dinamik ölçeklenebilen altyapısı, farklı coğrafyalara yayılan veri merkezleri, kaynaklarının çok sayıda kullanıcı arasında paylaşılarak kullanılması gibi özelliklerinden dolayı bulut ortamında yapılan adli soruşturmalar daha karmaşık bir hâl almaktadır. Geleneksel adli bilişim yaklaşımı bulut bilişim ortamında karşılaşılan sorunları tam olarak çözümleyemediği için; adli bilişime, buluta doğru genişleyen yeni bir bakış kazandırmaya yönelik çalışmalar yapılmaktadır.

Bulut adli bilişim, bulut bilişim ile dijital adli bilişimin kesişim noktasında, ağ adli bilişimin bir alt parçasıdır. Ağ adli bilişim, bilgisayar ağları üzerinde yapılan adli soruşturmalar ile ilgilidir. Bulut bilişimin de geniş bir ağ üzerine kurulu olmasından dolayı bulut adli bilişim, ağ adli bilişimin işleyiş sürecini temel alır [20].

Bulutun son derece esnek bir yapısı vardır. Bu nedenle bulut ortamında yapılan adli soruşturmalarda, delil toplamaya yönelik araç ve süreçlerin de aynı esneklikte olması gereklidir. Bulutun önemli bir karakteristiği de kaynakların, çok sayıda kullanıcı arasında paylaşılarak kullanılmasıdır. Bu nedenle soruşturmalar sırasında aynı fiziksel kaynak üzerindeki farklı kullanıcılardan yalnız soruşturmaya hedef olanın ayırt edilmesi gereklidir.

Soruşturma esnasında bulut bilişim hizmetlerinde herhangi bir aksamaya da meydan verilmemelidir.

A. Bulut Üzerinde Adli Bilişim Süreci

Dijital adli bilişim uygulamalarına temel oluşturmak üzere geliştirilen ISO 27037 standardına göre, adli bilişim sürecinde tanımlama, toplama ve koruma adımları yer alır. Buna ek olarak analiz, yorumlama ve raporlama adımları da sürece dâhil olmuştur.

Delili Tanımlama

Potansiyel dijital delilin fark edilip belgelendirilmesi için yapılan aramayı kapsayan süreçtir [22]. Bulut bilişim ortamında tanımlama süreci son derece karmaşık bir hâl alabilmektedir.

Bulut bilişim altyapıları, büyük ölçekli bir veri merkezi üzerinde çok sayıda depolama ve işlem kaynağının birbirine bağlanması ile meydana gelir. Hatta bulut bilişim platformları birden çok veri merkezini de birbirine bağlayarak çok sayıda kaynağı yekpare bir bütün olarak çalıştırmaktadır. Bulut ortamına aktarılan veriler, sistem içerisindeki dağıtım mekanizmaları tarafından çok sayıda depolama ve işlem kaynağı üzerine aktarılır. Bulut ortamında saklanan verilerin gerçek anlamda hangi konumda depolandıkları ve işlem gördükleri kullanıcılardan soyutlanmıştır. Bundan dolayı delil toplama sürecinde verinin bulunduğu konumun tespiti ve delilin elde edilmesi zorlaşmaktadır. Delillerin potansiyel konumlarına, servis sağlayıcıların sunduğu kayıtlar ya da çeşitli uygulama logları üzerinden elde edilen izlerle ulaşılabilmektedir.

Delil Toplama

Kanunlar çerçevesinde, potansiyel delil içeren unsurları derleme sürecidir.

Bulut mimarisinde veriler dağıtık bir altyapı ve sanallaştırılmış bir ortamda tutulduğundan dolayı delil toplama süreci zorlaşmaktadır. Çok sayıda kaynak üzerine dağılmış verilerin toplanıp, bütünlüğünün sağlanarak kabul edilebilir bir delil haline dönüştürülmesi kolay değildir. Bulut bilişimin sanallaştırılmış yapısından dolayı bir takım veriler belirli bir süre sonra yok olabilmektedir. Delil toplama aşamasında bu durumun da dikkate alınarak, işlemlerin son derece seri bir şekilde gerçekleştirilmesi gerekmektedir.

Koruma

Potansiyel dijital delilin bütünlük ve orijinal durumunun muhafaza edilmesi sürecini ifade eder [22]. Koruma, hukuk mahkemesinde delilin kabul edilebilirliğine etki eder. Dijital delillerin değiştirilmesi ya da yok edilmesi kolaydır. Bu nedenle koruma sürecinde, verilerin kazara ya da kasti bir şekilde değiştirilmesine karşı gerekli önlemler alınmalıdır.

Analiz

Potansiyel bir delil kaynağından elde edilen delil öğelerinin işlenmesi sürecidir [22]. Analiz, durağan ya da canlı olarak yapılabilir. Yinelemeli bir süreç olup, süreç içinde ortaya çıkan sorular yeni analiz süreçleri doğurabilir.

Yorumlama

Soruşturmayı gerçekleştirmek için, analiz ve incelemeler sonucu elde edilen verilerin sentezlenerek gerçeğe dayalı delilin ortaya çıkarılması sürecidir [22].

Raporlama

Analiz ve yorumlama sonucunda elde edilen sonuçların yazılı veya sözlü olarak sunumunu içine alan süreçtir.

B. Bulut Ortamından Delil Elde Etme ve Karşılaşılan Zorluklar

Bulut bilişim ortamlarında yürütülen adli soruşturmalarda, kullanılan bulut bilişim mimari modeline bağlı olarak çeşitli zorluklar ortaya çıkabilmektedir. Başka bir kuruluş tarafından yönetilen genel bulut mimarisi üzerinden delil elde etmek, bir kuruluşun kendi bünyesindeki özel buluta nazaran daha zordur [23].

Özel bulut mimarisinde bilgi teknolojileri altyapısı kuruluşun kendi bünyesinde yer almaktadır. Bu nedenle potansiyel delillerin araştırılacağı alan kapalı ve sınırlıdır. Genel bulut mimarisinde ise kamusal bir ağ üzerinde son derece geniş ve çok sayıda kullanıcının paylaştığı, dinamik olarak ölçeklenen bir altyapı vardır. Genel bulut mimarisinde veriler farklı ülkelerde yer alan veri merkezlerinde tutulabilir. Veriler, kullanım esnasında bir noktadan başka bir noktaya sürekli göç halindedir. Ayrıca verinin birden çok noktada kopyaları da bulunabilir. Bulut servisi üzerinde yer alan verilerin herhangi bir zaman diliminde hangi konumda tutulduğunu kestirmek zordur.

Sanallaştırılmış bulut ortamında yer alan bazı veriler uçucu nitelikte olabilmektedir. Bu da bir takım verilerin geri getirilemez olmasına neden olmaktadır.

Kamuya açık bir ağa, hassas verilerini göndermek bulut bilişim kullanıcılarını endişelendirmektedir. Altyapının internete açık olması, paylaşılarak kullanılan kaynaklar veri güvenliği üzerinde risk oluşturmaktadır. Bu nedenle kullanıcılar, verilerini bulut ortamına göndermeden önce şifreleme yoluna gitmektedir. Bu durum veri güvenliğini arttırmakta ancak, adli bilişim soruşturmalarında potansiyel delillerin çözümlenmesini zorlaştırmaktadır.

Genel bulut mimarisinde veriler ülke sınırları dışında yer alan veri merkezlerinde de tutulabilmektedir. Bulut hizmetinin kullanıldığı ülkede suç teşkil eden bir durum, iş sürecinin üzerinde gerçekleştiği veri merkezlerinin sınırları içinde bulunduğu ülke yasalarınca suç sayılmayabilir. Bu gibi durumlarda adli bilişim soruşturmaları ve uygulanacak yaptırımlar için uluslararası işbirliklerine gerek duyulmaktadır.

Bulut ortamından delil elde etme konusunda kullanıcıların yetenekleri, kullanılan bulut bilişim servis modeline bağlı olarak kısıtlılıklar göstermektedir. Kullanıcıların kısıtlandığı durumlarda bulut servis sağlayıcılardan talepte bulunulmaktadır. Kullanılan servis modeline bağlı olarak delil elde etme konusunda kullanıcılar ve servis sağlayıcıların olanakları şu şekildedir:

SaaS Modeli

SaaS modeli kullanıcıların delil elde etme yeteneği açıcından en kısıtlı olduğu modeldir. Hizmet kullanıcıları altyapının işleyen mekanizmaları (sunucular, işletim

sistemleri kaynak kodlar vs.) üzerinde kontrole sahip değildir. Bu durum kullanıcıların adli bilişim yeteneklerini de kısıtlar. SaaS ortamlarında adli bilişim araştırmacıları uygulama loglarına ve servis sağlayıcının sunduğu adli bilişim fonksiyonelliklerine güvenirler. Gerekli olan adli bilişim fonksiyonellikleri, kullanıcılar ile servis sağlayıcılar arasında yapılan servis düzeyi anlaşmaları (SLA) içerisinde belirtilmektedir.

PaaS Modeli

PaaS modelinin en büyük avantajlarından biri; hizmet kullanıcılarının, geliştirilen uygulamayı ve kaynak kodları kontrol etme yeteneğine sahip olmalarıdır. Bu durumda kullanıcılar, uygulamaların içerisine adli bilişim yeteneklerini (otomatik log mekanizmaları vs.) yerleştirebilirler. Kullanıcılar uygulamanın fonksiyonelliğini kontrol etme gücüne sahip olmakla birlikte, uygulamanın çalışması yine servis sağlayıcı altyapısında gerçekleşmektedir. Bu nedenle, PaaS modelinde, kullanıcı ve servis sağlayıcılar arasında bir koordinasyona gerek duyulur.

IaaS Modeli

SaaS ve PaaS ile kıyaslandığında IaaS, büyük bir delil elde etme potansiyelini kullanıcıların kontrolüne sunar. Kullanıcılar, altyapı kaynaklarına daha çok müdahile edip ve bu kaynaklardan veri elde edebilmektedir. Bunun yanında bazı, belki de çok kritik veriler servis sağlayıcı altyapısında ve onun kontrolündedir. Bu nedenle, yine kullanıcılar ve servis sağlayıcılar arası bir koordinasyon gereklidir.

C. Servis Düzeyi Anlaşması (Service Level Agreement – SLA)

Bulut bilişim servis sağlayıcıları ile hizmet kullanıcıları arasında, hizmetin sürekliliği ve güvenliğini garanti eden "Servis Düzeyi Anlaşması" (SLA) yapılır [16]. Bu sayede tarafların sorumlulukları belirlenmiş, hizmette süreklilik ve erişilebilirlik garanti edilmiş olur.

Bulut ortamında yapılacak soruşturmalar servis sağlayıcılar ile kullanıcılar arasındaki bu karşılıklı anlaşmalar ve yasal düzenlemelere bağlıdır. Bulut servis sağlayıcılar ile kullanıcılar arasında yapılan SLA, herhangi bir soruşturma anında kullanıcı ve servis sağlayıcının yükümlülüklerini belirler.

D. Bulut Bilişim Ortamında Adli Soruşturma Prosedürleri

Bulut bilişim ortamındaki adli soruşturmalarda ilk göz önünde bulundurulması gereken, hangi bulut bilişim mimari modelinin kullanıldığıdır [7]. Modele bağlı olarak sürecin işleyişi farklılık gösterir. Özel bulut yapısında veriler bir kuruluşun kendi bünyesindeki ya da bir dış destekçinin bilgi işlem altyapısındaki sunucularda yer alır. Ayrıca soruşturma sırasında, kilit isimler olan sistem yöneticisi ya da çalışanlarına da ulaşmak kolaydır.

Kamusal ölçekte bir bulut ortamında işler daha karmaşık hale gelir. Bu ortam dinamiktir ve ihtiyaca göre şekillenebilmektedir [2]. Kullanıcı, tek bir mantıksal konuma erişiyor gibi görünürken arka planda çok sayıda uygulama ile görünmez bir şekilde etkileşim halindedir. Arka plandaki bu görünmez etkileşim ve dağıtım potansiyel delil kaynaklarının tanımlanmasını karmaşıklaştırır.

Soruşturma sırasında altyapıdaki tüm cihazların yerinde ve çalışır vaziyette olması gerekir. Bulut altyapısında veriler farklı konumlarda depolandıkları için her hangi bir sunucunun aktif olmaması delil bütünlüğünü bozabilir.

Bulut ortamında soruşturmaya ilişkin verinin aranacağı geniş bir altyapı olmasına karşı kaynakların erişilebilir olduğu zaman dilimi kısıtlıdır. Bu nedenle araştırmaların son derece planlı ve seri bir şekilde yürütülmesi gerekmektedir.

Kamusal bulut üzerinde adli soruşturma yaparken bulut hizmetinin işleyişi aksatılmamalıdır. Soruşturma esnasında hedefte olmayan diğer kullanıcılar herhangi bir zarara uğratılmamalıdır.

Adli bilişim sürecinde kişisel verilere erişim, kanunlar çerçevesinde gerçekleşir. Soruşturma sırasında bu verilere nasıl ulaşılacağı ve nasıl işleneceğini yasalarca belirlenir ve kişisel veriler koruma altına alınır. Veriler yalnız soruşturma ekibi tarafından incelenebilir, üçüncü şahıslar tarafından görülemez.

V. TÜRKİYE'DE BULUT BİLİŞİM VE ADLİ BİLİŞİM

Son yıllarda hızlı bir gelişim gösteren bulut bilişime yönelim ülkemizde de hızla artmaktadır. Telekomünikasyon, bankacılık, elektronik belge yönetimi gibi pek çok alanda bilgi teknolojileri altyapıları buluta doğru genişlemektedir. Ülkemizde bulut hizmeti veren servis sağlayıcıların sayısı da her geçen gün artmaktadır. 2013 yılı bitimine kadar küresel pazarda bulut hizmetlerindeki büyümenin yüzde 26 seviyesine ulaşacağı, Türkiye'deki büyümenin ise yüzde 54 civarında artacağı tahmin edilmektedir [24].

Bilişim sektöründeki hızlı gelişmeye paralel olarak bilişim alanında işlenen suçların sayısı da giderek artmaktadır. Türkiye dışındaki pek çok ülke daha erken dönemlerde adli bilişim faaliyetlerini başlatmışken, ülkemizde 2006 yılından itibaren aktif anlamda adli bilişim çalışmaları başlamıştır [25].

Ülkemizdeki adli bilişim faaliyetleri gün geçtikçe hızlanmakta, resmi kurumlar ve dernekler adli bilişim konusundaki çalışmalarına ivme kazandırmaktadır. Ancak adli bilişim konusunda ülkemizde yürütülen çalışmalar henüz yeterli seviyede olmayıp bilhassa yeni şekillenen teknolojik gelişmelere paralel ilerlemelerde eksiklikler mevcuttur. Küresel ölçekte bulut bilişim alanında yürütülen adli bilişim çalışmaları da yeni yeni şekillenirken, ülkemizde bulut adli bilişim konusunda henüz önemli bir adım atılmamıştır. Bu anlamda Türkiye'deki adli bilişim çalışmalarına ve çağın teknolojisi olan bulut adli bilişim konusundaki çalışmalara daha çok önem verilmeli ve hız kazandırılmalıdır.

VI. SONUÇ

Bulut bilişim sunduğu olanaklarla günümüzün yaygın kullanılan teknolojilerinden biri haline gelmiştir. Ancak, sunduğu olanakların yanında bir takım güvenlik risklerini de beraberinde getirmektedir. Bulutun sanallaştırılmış, dağıtık

ve paylaşılan altyapısı kullanıcıların veri güvenlik ve gizliliği konusundaki kaygılarını arttırmakta ve bu konuda işlenecek bilişim suçlarına açık kapı bırakmaktadır. Bulut bilişim servis sağlayıcılarının veri merkezlerini farklı ülkelere konuşlandırmaları, veriler üzerinde sınırları içerisinde bulundukları ülkenin yasalarını geçerli kılmaktadır. Ülkelerin veri güvenliği konusundaki yasal boşlukları ve bulut bilişimin sunduğu diğer açık kapılar, bilişimin suçlularını bulut platformlarına doğru çekmektedir. Bulut üzerinde işlenen adli suçların artması ve geleneksel adli bilişim yaklaşımının bulut bilişimi tam anlamıyla kapsamıyor oluşu, adli bilişimin bulut bilişime özgü olarak yeniden yapılanmasını gerektirmiştir. Bulut bilişim sistemlerinden dijital delil elde etmek geleneksel sistemlere nazaran daha karmaşıktır. Adli soruşturmalarda delil elde etme konusunda bulut servis sağlayıcıları ve hizmet kullanıcıları arasındaki karşılıklı sorumluluklar ve koordinasyon önemlidir. Servis sağlayıcılar ve kullanıcılar arasında yapılan servis düzeyi anlaşmaları, tarafların sorumluluklarını belirler. Herhangi bir adli soruşturmada delil elde etme konusunda bulut müşterileri çok sıkıntı yaşadıkları için doğru servis sağlayıcının seçimi büyük önem taşımaktadır. Soruşturma esnasında verilen hizmetinin aksamadan devam etmesi, soruşturmanın hedefinde olmayan kullanıcıların etkilenmemesi, verilerin gizliliğinin korunması gerekmektedir.

KAYNAKLAR

[1] Cloud Security Alliance," Mapping the Forensic Standart ISO/IEC 27037 to Cloud Computing", June 2013.
[2] B. Treacy, "Cloud computing: data protection concerns unwrapped", Privacy and Data Protection, vol. 9(3), 2009, pp. 1-3.
[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Brobery, I. Brandic "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", Future Generation Computer Systems, vol. 25(6), 2009, pp. 599-616.
[4] M. Taylor, J. Haggerty, D. Gresty, R. Hegarty, "Digital evidence in cloud computing systems", Computer Law & Security Review, vol. 26, 2010, pp. 304-308.
[5] Y. Zhang, A. Juels, M. Reiter, T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys", In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). ACM, New York, 2012, pp. 305-316.
[6] T. Risenpart, E. Tromer, H. Shacham, S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds" In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). ACM, New York, 2009.
[7] M. Taylor, J. Haggerty, D. Gresty, D. Lamb, "Forensic investigation of cloud computing systems", Network Security, vol. 2011, 2011, pp. 4-10.
[8] E. Casey, "Cloud computing and digital forensics", Digital Investigation, vol. 9, 2012, pp. 69-70.
[9] H. Chung, J. Park, S. Lee, C. Kang, "Digital forensic investigation of cloud storage services", Digital Investigation, vol. 9, 2012, pp. 81-95.
[10] M.G. AHI. (2009, Mart) ."Adli Bilişim Nedir?". *Güncel Hukuk* [Online]. Erişilebilir: http://www.guncelhukuk.com.tr/dergi/
[11] J.F. Rayport, A. Heyward. (2009)." Envisioning the Cloud: The Next Computing Paradigm". *MarketspaceNext* [Online]. Available: http://marketspacenext.com/inthemedia/envisioning-the-cloud/
[12] E. Knorr, G. Gruman. (2008)." What cloud computing really means". *InfoWorld* [Online]. Available: http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031
[13] F. Chong, G. Carraro. (2006, April) ."Architecture Strategies for Catching the Long Tail". *MSDN* [Online]. Available: http://msdn.microsoft.com/en-us/library/aa479069.aspx
[14] T.V. Lillard, C.P. Garrison, C.A. Schiller, J. Steele, *The Future of Cloud Computing*. Boston: Elseiver Inc., 2010, ch.12.
[15] M. Çelik.(2009, Ekim). "Neden Sanallaştırma?".*Bilisim News* [Online]. Erişilebilir: http://www.bilisimnews.com/?p=475
[16] S. Krishnan, *Programming Windows Azure*. USA: O'Reilly Media, 2010.
[17] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol.34 (1), 2011, pp. 1-11.
[18] D. Svantesson, R. Clarke, "Privacy and consumer risks in cloud computing", Computer Law & Security Review, vol. 26 (4), 2010, pp. 391-397.
[19] Y. Korkmaz.(2010, Haziran). "Bulut Bilişim Risk Değerlendirmesi – I". *Tübitak Bilgem* [Online]. Erişilebilir: http://www.bilgiguvenligi.gov.tr/ guvenlik-teknolojileri/bulut-bilisim-risk-degerlendirmesi-i.html
[20] K. Ruan, J. Carty, T. Kechadi, M. Crosbie, "Cloud Forensic", IFIP Advances in Information and Communication Technology, vol. 361, 2011, pp. 35-46.
[21] X. Li, J. Seberry, "Forensic Computing", in *Proc. 4th International Conference on Cryptology in India, New Delhi, India, 2003*, pp.18–35.
[22] *ISO 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence*, ISO/IEC 27037, 2012.
[23] R. Grossman,"The case for cloud computing", IT Professional, vol. 11(2), 2009, pp. 23-27.
[24] Capital Online. (2012, Eylül) ." Türkiye'de Bulut 2013'te yüzde 54 büyüyecek". Capital İş & Ekonomi [Online]. Erişilebilir: http://www.capital.com.tr /turkiyede-bulut-2013te-yuzde-54-buyuyecek-haberler/24990.aspx
[25] S. Kurt.(2011, Aralık). "Adli Bilişim ve Türkiye'de Adli Bilişim". *Çözüm Park* [Online]. Erişilebilir: http://www.cozumpark.com/forums/thread/290988.aspx

Onur SEVLİ, 1987 yılında Isparta'da doğdu. Lisans eğitimini Süleyman Demirel Üniversitesi, Teknik Eğitim Fakültesi, Elektronik-Bilgisayar Eğitimi Bölümün'nde 2009 yılında tamamladı. Yüksek lisans eğitimini, Süleyman Demirel Ünivesitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı'nda 2011 yılında tamamladı. Aynı yıl Süleyman Demirel Ünivesitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Mühendisliği Ana Bilim Dalı'nda doktora eğitimine başladı. Doktora süreci, tez aşamasında devam etmektedir. Halen Mehmet Akif Ersoy Ünivesitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Bölümü'nde öğretim görevlisi olarak çalışmaktadır. Yazılım, bilişim ve güvenlik konularında çalışmalar yapmaktadır.

Ecir Uğur KÜÇÜKSİLLE, 1976 yılında Isparta'da doğdu. Gazi Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği lisans eğitimini tamamladı. Yüksek lisans eğitimini Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Makine Eğitimi Ana Bilim Dalında yaptı. Doktora eğitimini Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü İşletme/Sayısal Yöntemler Ana Bilim Dalında tamamladı. Halen Süleyman Demirel Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır. Bilgisayar, güvenlik ve yapay zeka alanlarında çalışmaları bulunmaktadır.