ADLİ BİLİŞİM EZBERLERİNİ BOZAN BİR DÜZLEM: BULUT BİLİŞİM

Adem EMEKCİ[1], Emin KUĞU[1], Murtaza TEMİZTÜRK[2]
[1]Havacılık ve Uzay Teknolojileri Enstitüsü - Hava Harp Okulu, İstanbul, Türkiye
[2]Savunma Bilimleri Enstitüsü - Kara Harp Okulu, Ankara, Türkiye
adem.emekci@gmail.com , e.kugu@hho.edu.tr, mtemizturk@kho.edu.tr

ÖZET

Adli bilişim alanı her geçen gün çok çeşitli problemlerle karşılaşmaktadır. Özellikle suç vakalarında müdahale edilen büyük veri, yaygın olarak kullanılan kriptografik uygulamalar, mobil teknolojilerdeki muazzam gelişim ve yasaların teknolojik yeniliklere cevap vermede geç kalması bunların başlıcaları olarak sıralanabilir. Bulut bilişim teknolojilerinin hayatımıza iyiden iyiye nüfuz etmeye başladığı günümüzde, artık her işlem sadece internete bağlanma uzaklığındadır. Bilişim teknolojilerinin küreselleşmesine katkısı büyük olan bulut bilişim, bu yönüyle bilişim evriminin son halkasını oluşturmaktadır. Bu çalışmanın konusu, adli bilişim dünyasının yürümek zorunda olacağı belki de en engebeli yol olacak bulut adli bilişimidir. Bulut bilişimin hayatlarımızı ve çalışmalarımızı kolaylaştırdığı ortadayken, adli bilişim dünyasındaki yansımaları ise şimdilik ters yöndedir. Çalışmamızda ağırlıklı olarak bulut adli bilişiminin getirdiği açmazlar, buna ilaveten sınırlı olarak da bulut bilişim teknolojilerinin adli bilişim alanına getirdiği avantajlar üzerinde durulmuştur.

Anahtar Kelimeler: Adli bilişim, Bulut adli bilişimi, Bulut bilişim, Bulut bilişim teknolojileri.

THE DOMAIN BREAKING THE MOLDS OF DIGITAL FORENSICS: CLOUD COMPUTING

ABSTRACT

Digital forensics world everday faces miscellaneous problems. Especially vast amount of data regarding the cases, common usage of cryptographic applications, the huge progress in mobile technologies and the latent reaction of legal regulations to new technological developments can be listed as the principal issues. Due to massive infiltration of cloud technologies into our lives, it's just internet connection we need. Cloud computing is the last ring of the computing evolution, due to its massive contribution to the globalization of IT technologies. The main issue of this paper is cloud forensics, maybe the roughest road on which digital forensics has to walk. It's obvious that cloud computing facilitates our lifes and efforts, but for now it's just the reverse for digital forensics. In the paper, we focused mainly on the challenges of cloud forensics, and on a limited basis the advantages of cloud computing on digital forensics.

Keywords: Digital forensics, Cloud forensics, Cloud computing, Cloud computing technologies.

I. GİRİŞ (INTRODUCTION)

Günümüzde problem alanı giderek genişleyen adli bilişim dünyası, bulut bilişimin getirdiği paradigma değişimiyle neredeyse tüm bildiklerini unutma ve yeni çözümler bulma noktasında görünmektedir. Bulut bilişim teknolojilerinin çok dinamik bir yapıda olması, adli bilişim için zorunluluk arz eden "kim, ne amaçla, ne zaman, nerede, nasıl, ne yapmış?" sorularının cevaplarını bulmayı çok zorlaştıran bir mahiyet sergilemektedir. Adli bilişim dünyasının, belki de üstesinden gelmesi gereken en zor teknoloji değişimiyle karşı karşıya olduğunu söyleyebiliriz.

Bilişim teknolojilerindeki bu büyük devrimin, görünen o ki adli bilişim dünyasındaki karşılığı ancak bir bakıcı ifadesiyle "bunca yaramaz çocukla baş etmeye çalışırken, bir tek sen eksiktin" olabilir. Her ne kadar, 1990'larda kişisel bilgisayarlar (PC) ile başlayan, 2000 yılı başlarından itibaren internet teknolojileri ile devam eden bilişim devriminin son halkasında, 2010'dan başlayarak üçüncü on yılın yıldızı olarak bulut bilişim teknolojileri gösterilse de [1], zaten birçok kaynaktan gelen zorluklarla başa çıkmaya çalışan adli bilişim dünyası için, bu son halkanın etkisinin kırılması çok zaman alacak gibi görünmektedir.

Bulut bilişim teknolojilerinin, adli bilişim alanına negatif etkisinin uzun süre devam edeceğini öngörmemizin temel nedeni, özellikle bulut bilişim teknolojilerinin güvenlik açısından tam olarak olgunluğa erişememiş olması ve bulut teknolojilerinin adli bilişim uygulamalarını pek dikkate almayan bir istikamette ilerlemesidir. Önümüzdeki süreçte görünen o ki, bulut bilişim teknolojileri, en azından genelgeçer araç, yöntem ve uygulamalar geliştirilene değin, adli bilişim dünyasının baş etmekte çeşitli açmazlarla karşılaşacağı ve tabiri caizse ezberlerin bozulduğu bir düzlem olacaktır.

Bu çalışmamızda; ağırlıklı olarak bulut bilişim teknolojilerinin adli bilişim alanına getirdiği problem sahalarını ve sınırlı olarak da bulut bilişim teknolojilerinin adli bilişim alanına getirdiği avantajları ele aldık. Çalışmamızın müteakip bölümleri ve ele alınacak konular şöyledir: Bölüm 2'de bulut bilişim teknolojileri, Bölüm 3'te adli bilişim ve bulut adli bilişimi kavramları ve Bölüm 4'te bulut bilişim teknolojilerinin adli bilişim alanına etkileri ele alınacak, Bölüm 5'te problem alanlarının giderilmesi noktasında bir değerlendirme yapılarak sonuç ortaya konulacak ve çalışma tamamlanacaktır.

II. BULUT BİLİŞİM KAVRAMI (CLOUD COMPUTING)

A. Bulut Bilişim Kavramı ve Özellikleri (Cloud Computing and Characteristics)

Özellikle mobil iletişim platform ve ortamlarındaki gelişmeler, iş dünyasının çok dinamik bir yapıda olması ve sürat gerektirmesi, devletlerin ve ticari girişimcilerin bilişim teknolojilerine yaptıkları yatırımların yeni ürün ve teknolojiler ile artması gibi nedenler, bulut bilişim kavramını ve teknolojilerini doğurmuştur. Bilişim dünyasının bu sınırları zorlayan yeni çocuğunun dünyamızın küreselleşmesi benzeri, bilişim teknolojilerinin yaşamakta olduğu evrimin son halkası olduğunu ifade edebiliriz.

Bulut bilişim kavramı, Türk Standartları Enstitüsü'nce hazırlanan dokümanda [2] "işlemci gücü ve depolama alanı gibi bilişim kaynaklarının ihtiyaç duyulan anda, ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve veriye izin verilen her yerden kontrollü erişimin mümkün olduğu, gerektiğinde kapasitenin hızlı bir şekilde arttırılıp azaltılabildiği, kaynakların kullanımının kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür" şeklinde tanımlanmıştır.

Yine Amerikan Ticaret Bakanlığı bünyesindeki Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology - NIST), bulut bilişim kavramını, "paylaşımlı ve ayarlanabilir bir kaynaklar havuzuna (ağlar, sunucular, depolama ortamları, uygulamalar ve diğer hizmetler), internet bağlantısı üzerinden istenilen her yerden ve uygun bir şekilde erişim imkânı veren ve minimum seviyede yönetimsel çaba ve hizmet sağlayıcıların desteği ile süratli bir şekilde hizmetlerin kullanıma sunulmasına imkân veren bir model" olarak tanımlamıştır [3].

Aynı enstitü tarafından, bulut bilişimin olmazsa olmazları ya da bir bilişim sistemine bulut bilişim teknolojisi denebilmesi için gereken özellikler; istendiğinde kendiliğinden hizmete erişim, geniş ağ bağlantısı, kaynakların bir havuzda birleştirilmesi ve bu havuz aracılığıyla dağıtımı/kontrolü, süratli bir şekilde hizmetin esnetilebilmesi ve verilen/alınan bu hizmetlerin ölçülebilir olması olarak belirlenmiştir. Şekil-1'de bulut bilişim genel mimarisi görülmektedir.

B. Hizmet Türleri (Service Models)

1. Bulut Yazılım Hizmeti (Software-as-a-Service)

Kullanıcıların, sadece bulut hizmet sağlayıcısı tarafından kendilerine bir bulut altyapısı üzerinden sunulan yazılımları internet bağlantısı olan herhangi bir cihaz vasıtasıyla bir arayüz ya da bir tarayıcı aracılığıyla kullanabildiği ve kullanıcıların yazılımlar üzerinde sınırlı ayarlamalar gerçekleştirebildiği bulut bilişim mimarisidir. Kullanıcılar açısından temel hedef, donanım, yazılım, bakım ve idame ile personele ayrılan giderlerin azaltılmasıdır.

2. Bulut Platform Hizmeti (Platform-as-a-Service)

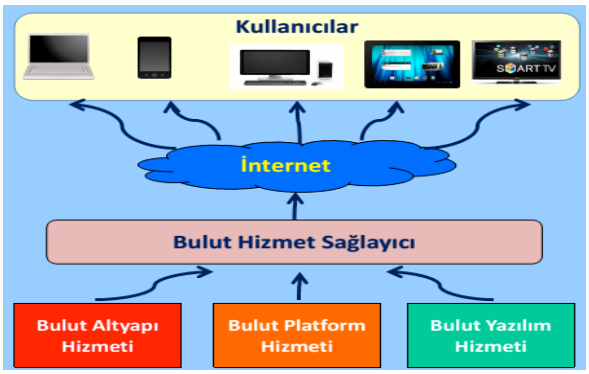
Kullanıcıların, bulut hizmet sağlayıcısı tarafından kendilerine bir bulut altyapısı üzerinden sunulan yazılım geliştirme ortamlarında kendi yazılımlarını geliştirebildikleri ve geliştirilen yazılımlar üzerinde kontrol ve denetim yapabildikleri bulut bilişim mimarisidir. Kullanıcılar açısından temel hedef, donanım ve yazılım temin etme giderlerinin azaltılmasıdır.

3. Bulut Altyapı Hizmeti (Infrastructure-as-a-Service)

Kullanıcıların, bulut hizmet sağlayıcısı tarafından kendilerine bir bulut altyapısı temelinde sunulan

altyapı üzerinden; işlemci gücü, bilgisayar ağları, veri depolama ortamları, işletim sistemleri ve üzerinde koşturulan uygulamalar gibi diğer temel bilişim kaynaklarını kullanabildikleri ve bahsedilen ortamlar üzerinde kontrol ve denetim yapabildikleri bulut bilişim mimarisidir. Kullanıcılar açısından temel hedef, donanım ve yazılım temin etme ve bunlar için belirli bir yer tahsis etme giderlerinin azaltılmasıdır [2]-[3].

Temel hizmet türleri yukarıda görülen üç tip olmakla birlikte, özellikle bulut güvenlik hizmeti (Security-as-a-Service), bulut adli bilişim hizmeti (Forensics-as-a-Service), bulut veritabanı hizmeti (Database-as-a-Service) gibi hizmet türleri de kullanıcıların ihtiyaçları doğrultusunda ortaya çıkmaktadır.



Şekil 1. Bulut bilişim mimarisi (The structure of cloud computing)

C. Dağıtım Modelleri (Deployment Models)

1. Özel Bulut Modeli (Private Cloud)

Genellikle güvenlik gereksiniminin ön planda olduğu organizasyonlar, Ar-Ge faaliyetlerine odaklı ya da kritik bir sektörde faaliyet gösteren ticari firmaların kullanageldiği bir modeldir (bir üniversite içerisinde konuşlu öğrenci pansiyonunda sadece okul öğrencilerinin kalabilmesi ya da bir firma mensuplarının gittikleri yerlerde anlaşmalı bir otelde kalmaları gibi). Kullanıcılar organizasyon içerisindendir ve mülkiyeti, yönetimi, işletimi ilgili kullanıcıda olabileceği gibi bu işi yapan üçüncü bir hizmet sağlayıcıda da olabilir. Ayrıca, kullanılan donanım ve istasyonlar kullanıcı bünyesinde tesis edilmiş olabileceği gibi dış kaynaklı da olabilir.

2. Genel Bulut Modeli (Public Cloud)

İsteyen herkese açık model türüdür. İster ticari bir firma, ister devlet kontrolünde bir yapı olsun kullanılacak altyapı, ilgili organizasyon dışında hizmet sağlayıcının işletim sorumluluğu ve denetiminde bir yerdedir. (bir ülkedeki yerli ya da yabancı turistlerin gittikleri tatil beldesindeki ya da şehirdeki istedikleri otelde kalabiliyor olmaları gibi)

3. Topluluk Bulut Modeli (Community Cloud)

Kullanım amacı yönünden özel bulut modeline; işletim sorumluluğu, yerleşim ve denetim açılarından ise genel bulut modeline benzeyen bir yapıdadır. (farklı bir şehirde düzenlenen bir seminere giden öğretmenlerin, o şehrin öğretmenevinde kalmaları ya da devlet memurlarının kendileri için tahsis edilmiş lojmanlarda kalması gibi)

4. Karma Bulut Modeli (Hibrid Cloud)

Yukarıda bahsedilen özel, genel ve topluluk bulut modellerinin karışımından oluşan bir modeldir. Her alt model kendi içerisinde kendi özelliklerini korur (bir üniversite kampüsü içerisinde; okulda görev yapan personelin kullanımı için ayrılan bir otopark, öğrencilerin kullanımına ayrılan bir otopark ve üniversiteye gelen misafirler için ayrılan otoparklar olduğunu, bunlar dışında üniversite sınırları içerisindeki bir Ar-Ge merkezinde çalışmalar yapan ve çeşitli üniversiteler ve ticari firmalardan katılımların olduğu bir çalışma grubu için belirlenmiş bir otopark ve son olarak isteyen herkesin araçlarını park edebildiği bir kafeteryaya ait bir otoparktan oluşan karma yapı gibi) [2]-[3]-[4].

III. ADLİ BİLİŞİM KAVRAMI VE BULUT ADLİ BİLİŞİMİ (DIGITAL FORENSICS AND CLOUD FORENSICS)

Adli bilişim kavramının ortaya çıkması, bilişim ve bilgisayar teknolojilerinin gelişmesine ve suç işlemede bir unsur olmaya başlamasına paralel olarak 1980'li yılların sonlarına dayanmaktadır. Ancak adli bilişim uygulamalarından biri olan veri kurtarma işlemini de dikkate aldığımızda, aslında 1970'lerin ilk dönemlerine kadar gitmemiz gerekir [5]-[6]. İlk olarak farklı şekillerde ifade edilse de (forensic computing, computer forensics, cyber forensics etc.) sayısal verilerin birçok ortamda üretilir, işlenir ve tutulur olması düşünüldüğünde günümüzde gelinen nokta itibariyle adli bilişim kavramının tam karşılığı İngilizce tabiriyle "digital forensics" ifadesidir.

Günümüzde kullanılan ya da anlaşılması gereken şekliyle tanımlayacak olursak, adli bilişim; konusu suç oluşturan eylemlerde, bu suçlarla ilişkili kişilerin kullandıkları elektronik ortamlardan elde edilen sayısal verilerin, işledikleri suçlarla bağlantılarını ortaya çıkarmak ve suç delillerini ilgili adli makamlara sunmak amacıyla güvenlik birimleri ya da ehliyetli kişi/kurumlarca yapılan analiz işlemleri bütünüdür diyebiliriz. Şekil-2'de adli bilişime konu olan çeşitli sayısal delil ortamları görülmektedir.

Adli bilişim uygulamalarında yapılan işlemler birbirlerine çok yakın olmakla birlikte, işlenen suçun türü, söz konusu elektronik ortam, elektronik ortamın yapısı, delillerin kalıcı-uçucu olması, suç

şüphelilerinin uyguladıkları karartma teknikleri ve yapılan işlemlerin zamanı gibi faktörlere bağlı olarak farklı adli bilişim türleri ortaya çıkmıştır [7]-[8].

- Statik veri adli bilişimi (disk forensics)
- Canlı adli bilişim (live forensics)
- Ağ adli bilişimi (network forensics)
- Mobil cihaz adli bilişimi (mobile device forensics)
- Veritabanı adli bilişimi (database, log forensics)

Şekil 2. Geleneksel elektronik delil ortamları (Conventional digital forensics media)

Çalışmamızın içeriğini oluşturan ve bulut bilişim teknolojilerindeki gelişmelerle doğru orantılı olarak genişlemeye devam eden bir diğer adli bilişim türü olarak da bulut adli bilişimini (cloud forensics) sayabiliriz. Bulut adli bilişimi, mimarisi itibariyle ağlardan ve ağa bağlı cihaz ve sistemlerden oluşması nedeniyle ağ adli bilişiminin bir alt disiplini olarak kabul edilmektedir. Bir diğer yaklaşıma göre ise bulut bilişim ile adli bilişim karması bir disiplindir [9].

Bulut adli bilişimin, ağ adli bilişiminin bir alt türü olduğunu kabul etmekle birlikte; buluttaki veri depolama olanaklarındaki gelişim dikkate alındığında sabit veri adli bilişimi, özellikle sanallaştırma teknolojisinin çok yoğun olarak kullanıldığı bir arena olarak bulut bilişim ortamlarına müdahale dikkate alındığında canlı adli bilişim, kullanıcı ve hizmet sağlayıcı arasındaki iletişim teknolojisine dayanarak ağ adli bilişimi, mobil cihazlardaki olağanüstü artış, internet erişim hızlarının alabildiğine genişlemesi ve ucuzlaması noktaları dikkate alındığında mobil adli bilişim ve son olarak da özellikle bulut bilişim teknolojilerinin iki ana unsurundan biri ve belki de büyük abisi diyebileceğimiz hizmet sunucu tarafındaki günlük kayıtlarını (logs) düşündüğümüzde veritabanı adli bilişimi, sunulan/alınan bulut bilişim hizmetinin türüne göre bulut adli bilişiminin konusunu oluşturur. Kısaca ifade etmek gerekirse, bahsedilen türlerden oluşmuş karma, farklı, özgün bir adli bilişim türüdür.

IV. BULUT BİLİŞİM TEKNOLOJİLERİNİN ADLİ BİLİŞİM ALANINA ETKİLERİ (THE EFFECTS OF CLOUD COMPUTING TECHNOLOGIES ON DIGITAL FORENSICS)

A. Genel Bakış (Overview)

Bulut bilişim teknolojilerinin ve kullanım alanlarının muazzam bir hızla artması, kullanılan ortamları suçlular/suç örgütleri için de cazip hale getirmiştir. İnternet kullanımındaki artış ve süratli erişim imkânları, kullanıcıların bilgisayar, tablet ya da akıllı telefonlar üzerinden bir tarayıcı ile istedikleri internet kaynağına ulaşmaları internet ortamını ve dolayısıyla da bulut bilişim ortamlarını özellikle siber suçlar ve hatta sunduğu depolama imkânları ile klasik suçlar için elverişli yeni bir saha haline getirmiştir [10].

Konuyu siber suçlar noktasında ele aldığımızda, güvenlik açısından henüz istenen olgunluğa erişememiş bir yapı olan bulut bilişim teknolojileri, siber korsanlar için bulunmaz bir ortam sunmaktadır. Hakeza, siber korsanlık marifetiyle ele geçirdikleri verileri muhafaza etmek için de bulut bilişimin sunduğu depolama imkânlarından daha iyi bir seçenek olamaz. Hatta özellikle son dönemlerde hayli dikkat çeken, firmalara ya da firmaların işlemlerini gerçekleştirirken kullandıkları gerçek kişilere ait özel verilerin ele geçirilmesi, daha sonra bu verilerin çok kuvvetli kriptografik tekniklerle şifrelenerek bulutta bir yerlerde tutulması ve muhataplara para karşılığında şantaj yapılması konunun önemini çok açık bir şekilde gözler önüne sermektedir. Öte yandan, bulut bilişim depolama imkânları klasik suçlara ilişkin verilerin de muhafaza edilebilmesi noktasında büyük kolaylıklar sağlamaktadır.

Mademki bahsettiğimiz suçlar bulut bilişim teknolojilerinin sunduğu ortamlarda işlenmektedir; tespit edilen suçların ve delillerin ortaya çıkartılması ve suçluların cezalarını almalarının sağlanması için neyin nasıl yapılacağının belirlenmesi ve gerçekleştirilmesi gerekmektedir. Maalesef bulut adli bilişimi, adli bilişimin şimdiye kadarki ilerlediği noktanın çok ilerisinde açmazlar getirmiştir.

Söz konusu açmazlar, birçok araştırmacı ve sahada aktif olarak görev yapan adli bilişim emektarı tarafından çeşitli araştırma ve makalelerde ele alınmıştır. Kimileri bu açmazları teknik, yasal ve organizasyonel boyutlarıyla ele almıştır [9]. Bazıları, klasik adli bilişim süreçlerinden yola çıkarak ilgili safhalardaki problemleri ortaya koyma yoluna gitmiştir [10]-[11]-[12]. Konuya ilişkin en kapsamlı çalışma Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından hazırlanmıştır. Haziran 2014'te taslak olarak yayımlanan dokümanda, bulut adli bilişiminin getirdiği söz konusu açmazlar, hem tekil olarak ve hem de birbirleri ile bağlantıları

noktasında üst gruplandırmalar şeklinde özetlenmiştir [13].

B. Bulut Adli Bilişimi ve Getirdiği Açmazlar (Cloud Forensics and The Challenges)

Bulut bilişimin getirdiği açmazların ve birbirleriyle bağlantılarının daha iyi anlaşılması açısından, bu açmazların organizasyon, yasal düzenlemeler ve teknik boyutları ile ele alınmasının daha uygun olduğu değerlendirilmektedir.

1. Organizasyonel boyuttaki açmazlar

a. Yapılan işlemlerin takibindeki zorluklar: Bulut teknolojilerinin yapısından kaynaklanan bir problemdir. Bir tarafta hizmet sağlayıcı, diğer tarafta kullanıcıların olduğu bir ortamda; bir soruşturma/incelemenin yapılabilmesi ve sayısal delillerin kontrol edilebilmesi çok da kolay olmayacaktır.

b. Görev ve sorumluluklardaki belirsizlik: Bulut adli bilişiminde şayet sorumluluklar tam olarak belirlenmemişse yapılacak bir soruşturma/incelemede kriz ortamı oluşacaktır. Bulut bilişim hizmetleri sağlanır ve alınırken hazırlanan hizmet seviyesi anlaşmalarında (service level agreement - SLA) genellikle adli bilişim konusu göz ardı edilmektedir. Adli bilişim uygulamaları yapılması gerektiğinde de kimin, hangi işlemi, nasıl, kiminle işbirliği içinde yapacağı konusunda belirsizlikler ortaya çıkmaktadır. Sonuçta, bulut ortamında adli bilişim uygulamaları dikkate alındığında mutlaka hizmet sağlayıcı ve kullanıcıların da yardım ve işbirliğine ihtiyaç vardır.

c. Başkalarına bağımlılık: Bulut bilişim ortamlarındaki dağıtık yapı dolayısıyla, adli bilişim uygulamalarında mutlaka bir yerde gözün göremediği, elin ulaşamadığı noktalar olacak ve söz konusu alanlarda gerçekleştirilmesi gerekli işlemlerde başkalarına bağımlılık kaçınılmaz olacaktır. Burada hizmet sağlayıcı tarafındaki personel yanında, bir başka ülkedeki kolluk kuvveti ile de işbirliği ve koordinasyon gereken durumlar olacaktır. Yapılan çalışmaların neresinde olunursa olunsun, karşıdaki muhatabın istenilen işlemleri ne kadar doğrulukla yaptığı ya da yapılması gereken işlemleri yerine getirmeye ne kadar ehliyetli olduğu noktalarında yüzde yüz emin olmak ve yapılan işlemlere tamamiyle sahip çıkabilmek mümkün olmayacaktır.

d. Eğitim: Bulut adli bilişimi, bu alanda görev alacak herkesin yetkin olmasını gerektirmektedir. Sadece hizmet sağlayıcı tarafındaki teknik personel, adli bilişim işlemlerini yerine getiren kolluk görevlisi ya da hukuki zemindeki hakim, savcı, avukat değil; özellikle ABD'de olduğu gibi, adalet mekanizması içerisinde bulunan ve insanlardan oluşan jüri mensuplarının da konu hakkında belirli bir seviyede bilgi sahibi olması gerekmektedir. Sadece bir ya da birkaç tarafın konuya hakimiyeti olayın tam olarak anlaşılması ve net bir kanıya ulaşılması için yeterli olmayacaktır. Ancak en önemli görev ve sorumluluk kolluk görevlisinindir. Kolluk görevlisi, bir soruşturma sürecinde yaptığı uygulama ve işlemler ile eriştiği delilleri şeffaf bir şekilde muhataplara sunabilmeli ve karşı tarafı suçluluğa ya da suçsuzluğa ikna edebilmelidir.

Konuya ülkemiz özelinde bakacak olursak, karşılaştığımız manzara pek iç açıcı değildir. Ülkemizde bırakın bulut adli bilişimini, adli bilişim konusu özellikle akademik çevrelerde daha yeni yeni ilgi görmektedir. ABD, İngiltere, Avustralya gibi ülkelerde adli bilişim konusunda birçok standartlar oluşturulmuş, çeşitli eğitimler ve bu bağlamda sertifikalar belirlenmiştir. Ülkemizde ise maalesef birkaç makale okuyan bir akademisyen ya da üç-beş diskin kopyasını alıp inceleme yapan bir kolluk görevlisi kendisini bir anda adli bilişim uzmanı olarak lanse edebilmekte, bu durum ise bilirkişilik konusunun istismarına ve dolayısıyla da adaletin terazisinin şaşmasına neden olmaktadır.

2. Yasal boyuttaki açmazlar

a. Birden çok yasal alana yayılma: Yine bulut bilişim teknolojilerinin yapısı nedeniyle, sayısal deliller birçok yere dağıtık vaziyette bulunmaktadır. Delillerin elde edilmesindeki zorluklar yanında, ilgili verilerin bulunduğu yere bağlı olarak söz konusu takip edilen faaliyetin ilgili yerde suç olup olmadığı, yapılacak adli bilişim işlemlerinin hangi ülke yasaları çerçevesinde gerçekleştirileceği konuları ortaya büyük bir problemin çıkmasına neden olmaktadır. Unutulmamalıdır ki, yasalar çerçevesinde yapılmayan bir işlem boşa kürek çekmekten farksız olacaktır.

b. Çoklu kullanıcı profili ve diğer verilerin gizliliğine riayet problemi: Bulut adli bilişimin getirdiği en zorlu açmazlardan biri de bu konudur. Bulut bilişimin sanal teknolojilere dayanması, gerçekleştirilen soruşturma ve adli bilişim incelemelerini zorlaştıran bir etkiye sahiptir. Bulut hizmet sağlayıcıların birden çok kullanıcıya hizmet vermesi nedeniyle, gerçekleştirilen bir soruşturma ve adli bilişim incelemesi sadece ilgilisiyle sınırlı kalmamakta ve diğer kullanıcıların verilerine de erişim olmaktadır. Bu durum ise, hem elde edilecek sayısal delillerin sahihliğini tartışmalı hale getirmekte ve hem de konuyla hiç alakası olmayan özel/tüzel kişilerin verilerinin gizliliğine riayet edilmemesine neden olmaktadır.

c. Hizmet seviyesi anlaşmalarındaki eksiklikler: Bulut bilişim hizmetinden faydalanmak isteyen bir kullanıcı ile hizmet sağlayıcı arasında, hizmetin içeriği ve kapsamına ilişkin bir anlaşma yapılması gerekmektedir. Bu anlaşmaya hizmet seviyesi anlaşması (Service Level Agreement - SLA) adı verilmektedir. Çoğu zaman hizmet sağlayıcının asıl

amacı para kazanmak ve hizmetten faydalanmak isteyen kullanıcının da bir an önce işlerini yoluna koymak olduğundan, anlaşmanın adli bilişime ilişkin hususları göz ardı edilmektedir. Bu durum da, özellikle hizmet sağlayıcının konuyla alakalı bir hazırlığı yoksa ya da yeterli değilse, adli bilişim faaliyetlerinin gerçekleştirilmesi esnasında karmaşaya neden olmaktadır.

3. Teknik boyuttaki açmazlar

a. Delillerin toplanması ve elde edilmesi: Bulut adli bilişiminde en sorunlu konulardan bir tanesi de bu konudur. Geleneksel adli bilişim uygulamalarında, sayısal delilin bulunduğu bir ortam vardır ve öncelikle donanım açısından elektronik cihaza ulaşılması gereklidir ve bu aşama toplama olarak ifade edilir. Daha sonraki aşamada ise, elektronik cihazdaki sayısal deliller uygun yöntemlerle kopyalanır ve elde edilir. Bulut bilişim mimarisinde sanallaştırma uygulamaları yoğun olarak kullanıldığından, erişim çoğu zaman imkan dahilinde olmadığı için elektronik cihazların toplanması da pratikte mümkün olmamaktadır. Sayısal delillerin elde edilmesi, bahsedilen sanal uygulamalar ve sanal diskler üzerinden gerçekleştirilebilmektedir.

b. Verilerin dinamik yapısı: Bulut ortamındaki verilerin dağıtık bir yapıda olması, birden çok noktada birkaç kopyasının tutuluyor olması ve verilere ilişkin işlemlerin çok hızlı bir şekilde gerçekleşiyor olması adli bilişim uygulamalarını zorlaştırmaktadır.

c. *Delillerin ayrıştırılması:* Bir kullanıcı ile ilgili sayısal deliller elde edilmeye çalışılırken, örneğin bir sunucu üzerinde diğer kullanıcılara ait verilerin de depolanıyor ya da işleniyor olması, adli bilişim uygulamalarını zorlaştıracaktır. Bunun yanında yapılacak bir yanlış işlemle verileri ve faaliyetleri suç unsuru barındıran bir kullanıcı suçsuz, konuyla hiç ilgisi olmayan ve verilerini yasal çerçevede bulut ortamında tutan masum bir kullanıcı ise suçlu ilan edilebilecektir.

d. Verilerin yerinin tespiti: Geleneksel adli bilişimdeki elektronik ortamı tespit etme ve toplama mümkün olmadığı için bulut ortamındaki verinin tam olarak yerinin tespiti mümkün olamayabilmektedir. Ayrıca, verilerin yedeklenmesi de yaşanan sorunu katmerli hale getirmektedir.

e. Zaman farklılıkları ve deliller arasındaki korelasyonun sağlanamaması: Bulut ortamındaki çeşitli cihaz, sistem ve uygulamadan elde edilecek veriler arasındaki korelasyonun ortaya konabilmesi gerekmektedir. Bazen bir bulut hizmeti için belki bir hizmet sunucu, diğer bir hizmet sunucuya ve o da bir diğerine bağımlı durumda olabilecektir. Tüm bu hizmet sağlayıcılardan elde edilecek örneğin günlük kayıtlarının (logs) birbirleriyle hem format ve hem de zamanlama (synchronization) olarak ne kadar uyumlu olacağı büyük bir soru işaretidir. Buradan taşınan sorunlarla, örneğin bu kayıtlar ya da elde edilmiş başka veriler üzerinde, verilerin oluşturulma, değiştirilme ve hatta silinmelerine ilişkin olarak yapılacak bir analiz sağlıklı olmayacaktır.

f. Veri kurtarma: Geleneksel adli bilişim uygulamalarındaki gibi bir şekilde silinmiş, kaybolmuş verilerin kurtarılması ya da artıklarına ulaşılması, bulut ortamındaki kaynakların etkin kullanılması kapsamındaki esneklik ve dinamik yapı nedeniyle bulut adli bilişiminde pek mümkün değildir. Ancak, sanallaştırma uygulamalarının getirdiği anlık resim (snapshot) kabiliyeti adli bilişim uygulamalarına pozitif yönde bir etkiye sahiptir.

g. Şifreleme: Birçok bulut hizmet sağlayıcısı, kullanıcılara ait verilerin güvenilir bir yapıda tutulduğunu ve verilerinin gizliliğine riayet edildiğini garanti etme noktasında şifreleme (encryption) uygulamalarını kullanmaktadır. Yapılan bir adli bilişim uygulamasında şifrelenmiş verilerin çözümünün yapılabilmesi gerekmekte ve bu durum işlemleri zorlaştırmaktadır. Ayrıca, bunun haricinde kullanıcılara da verilerini şifreleme imkanı sağlanabilmekte, bu durumda ise elde edilen şifrelenmiş verilerin çözümlenebilmesi kullanıcının insafına ya da işbirliğine kalmaktadır.

C. Bulut Bilişim ve Getirdiği Avantajlar (The Advantages of Cloud Computing)

Bilişim evriminin son halkasını oluşturduğunu düşündüğümüz bulut bilişim teknolojilerinin, adli bilişim dünyasının başına sadece dert açtığını söylemek ve düşünmek her şeyden önce bilime ve gelişmeye aykırı bir çıkarım olacaktır. Mutlaka bulut bilişim alanındaki problem sahaları da zamanla azaltılacak ve belki de tamamen geçersiz kılınacaktır. Bulut bilişimin sunduğu imkânlar elbette adli bilişim faaliyetlerindeki diğer problemlerin giderilmesi noktasında kullanılabilmelidir.

Konuya ilişkin olarak ilk uygulama, henüz gelişme evresinde olan adli bilişim uygulamalarının bulut mimarisi üzerinden gerçekleştirilmesi düşüncesinden hareketle geliştirilen bulut adli bilişim hizmeti (Forensics-as-a-Service)'dir. Özellikle bilgisayar ve taşınabilir ortamlardan elde edilen sayısal delillerin depolanması ve analizinde işlemlerin hızlandırılmasına, delillerin daha güvenli bir ortamda tutulmasına ve adli bilişim uzmanları arasındaki fikir, bilgi, tecrübe alışverişine imkân sağlayarak işbirliğinin artmasına imkân sağlayacaktır. Diğer bir uygulama ise, özellikle kuvvetli şifrelerin kırılmasında bulut bilişimin işlemci gücünden yararlanılmasıdır.

Bahsedilen iki avantajdan farklı olarak, önceki kısımdaki açmazlar bir şekilde giderilir ve sağlıklı bir adli bilişim faaliyeti icra edilebilirse, bulut ortamındaki verilerin yedeklerinin bulunması ve birçok noktada kayıt bırakılması dikkate alındığında, bu durum özellikle bulut ortamında gerçekleştirilmiş siber suçlar soruşturulurken daha sağlıklı sonuçlara ulaşılmasında faydalı olabilecektir.

V. SONUÇLAR VE DEĞERLENDİRMELER (CONCLUSIONS AND EVALUATIONS)

Bulut bilişim teknolojileri şüphesiz bilişim dünyası için bir devrim niteliğindedir. Sürekli yeni çıkan ürünleri takip etmek, mevcut imkânlarını güncellemek durumunda kalan ve bu işlemler için büyük miktarlarda para ve emek harcayan iş dünyası, devletler ve hatta her birey için bulut bilişim teknolojileri ile bu problemler büyük ölçüde ortadan kalkacaktır. Bu kadar avantajları olan bir teknolojinin de günden güne kullanımının artarak yaygınlaşacağını tahmin etmek o kadar da zor değildir. Sistemlerini, faaliyetlerini, yaptıkları işlemleri bulut ortamına aktarmış olanlar için büyük bir kolaylıklar zaman dilimine girilmiştir. Bunun yanında birçokları için de buluta geçiş çok cazip görünmesine rağmen, özellikle güvenlik gerekçesiyle bu düşünceyi bir türlü hayata geçirememe durumu söz konusudur.

Bulut mimarisi itibariyle kolay erişilebilen, çok kuvvetli bir işlemci gücü sağlayan, neredeyse istenildiği kadar veri depolamaya imkân sunan ve yüksek mertebelerde ağ trafiğini kaldırabilen bir yapıdadır. Bu ortam yasal faaliyet yürütenler kadar, siber korsanların/ suç örgütlerinin de yaptıkları zararlı faaliyetleri için kaçırmak istemeyecekleri bir fırsattır. Güvenlik noktasında henüz tam olarak istenen seviyelerde bulunmayan bir zeminde, suça ilişkin faaliyetlerini kriptografik imkânlarla gizlemeleri, verilerini farklı bulut ortamlarında yedeklemeleri de çok kolay olmaktadır.

Suç işlemek için bu kadar müsait olan bir ortamda, suçların araştırılması ve gerekli delillerin elde edilmesi konusu da önemli bir yerde durmaktadır. Ancak bulut bilişim teknolojileri, adli bilişim açısından daha önceki seleflerine pek de benzemeyen bir seviyede zorluğu beraberinde getirmiştir. Henüz bulut ortamındaki bir sayısal delile tam olarak nasıl müdahale edilmesi gerektiği ile ilgili yetkin bir standart mevcut değildir. Aslında, her vaka kendi içinde ayrı bir vakadır. Tıp dünyasında şöyle bir ifade vardır: "hastalığa göre tedavi değil, hastaya göre tedavi uygulanması gerekir". Aynı durum bulut adli bilişimi için de geçerlidir. Bulut ortamında yapılan bir soruşturmanın ucunun nerelere kadar uzanacağı, sonuç alınıp alınamayacağı daha önce bahsi geçen nedenlerle muğlaklık arz etmektedir.

Sonuç olarak, bulut adli bilişimi hem bulut hizmeti sağlayıcılar, hem kolluk güçleri ve hem de yasal düzenlemeler noktasında içinde bulunduğu açmazlar yumağını çözmek durumundadır ve bu açmazların çözümünde sıralanan bileşenler dışında mutlaka akademik çalışmalara ve yeni yöntem ve araçlara ihtiyaç bulunmaktadır. Bu çalışmada sunulan ve bulut bilişimdeki açmazlar başlığı altında verilen hususlar dikkate alınmalı ve mutlaka uygun çözümler geliştirilmeye çalışılmalıdır.

VI. KAYNAKLAR (REFERENCES)

[1] C. Babcock, Bulut Bilişim İçin Yönetim Stratejileri, Koç Sistem Yayınları, İstanbul, 2010, pp.5.

[2] TSE, "Bulut Bilişim Güvenlik ve Kullanım Standardı", http://test.tse.org.tr/upload/tr/dosya/duyuruyonetimi/1082/12122014170015-2.pdf. (Erişim Tarihi: 25 Şubat 2015).

[3] P. Mell and T. Grance, The NIST Definition of Cloud Computing, 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. (Erişim Tarihi: 25 Şubat 2015).

[4] B. O. Okutucu, "Bulut Bilişim ve Teknolojileri," Yüksek Lisans Tezi, İstanbul, 2012, pp.51-52.

[5] S. L. Garfinkel, "Digital forensics research: the next 10 years," Digital Investigation, vol. 7, 2010, pp. S64–S73.

[6] I. Khoury and E. Caushaj, "Computer forensic", http://www.secs.oakland.edu/~iskhoury/Computer_Forensic_final.pdf. (Erişim Tarihi: 25 Şubat 2015).

[7] H. Önal, "Bilişim Sistemlerinde Adli Bilişim Analizi ve Bilgisayar Olayları İnceleme - 101", http://www.bga.com.tr/calismalar/computer_forensic101.pdf. (Erişim Tarihi: 25 Şubat 2015).

[8] J. Sammons, The Basics of Digital Forensics, Elsevier, USA, 2012, pp. 1-12.

[9] M. C. Keyun Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics : an overview", vol. 361, Springer, Berlin-Heidelberg, 2011, pp.35-47.

[10] D. Quick, B. Martini and R. Choo, Cloud Storage Forensics, Elsevier, USA, 2012, pp.1-12.

[11] J. L. Mauri, S. M. Thampi, D. B. Rawat, and D. Jin, Eds., "A heuristic model for performing digital forensics in cloud computing environment", vol. 467, Springer, Berlin-Heidelberg, 2014, pp. 341–352.

[12] G. Peterson and S. Shenoi, Eds., "Impact of cloud computing on digital forensic investigations", vol. 410, Springer, Berlin-Heidelberg, 2013, pp. 291–303.

[13] NIST Cloud Computing Forensic Science Challenges, http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf. (Erişim Tarihi: 25 Şubat 2015).