Bulut Bilişimde Bilgi Güvenliği ve Standardizasyon Çalışmaları

Gökhan Şengül, Atila Bostan

***Abstract*— Widespread usage and increasing speed of digital communication bring about proliferation and rising number of cloud applications which greatly depend on online information and service sharing. Although the technical qualifications have got quite close to user expectations, the principle problem of cloud services is still the security mechanisms between user and service provider, which have not reasonably matured yet. In forming the security mechanisms, dissemination of common standards is of great importance to provide grounds for common understanding and monitoring capability. Furthermore, these standards need to be published and necessary legal actions should be activated. This study aims to call attention to the importance of common security standards in cloud computing and provide a concise summary of ongoing standardization studies in Turkey. The study also points out the significance of cloud computing standards in e-government services.**

***Index Terms*— Security in cloud computing, Cloud computing standards.**

***Özet*— Sayısal iletişimin süratinin artması ve yaygınlaşması, ağ üzerinden hizmet ve veri paylaşım esasına dayanan bulut bilişim uygulamalarının da sayıca atması ve yaygınlaşması için ortam oluşturmaktadır. Teknik yeterliliği kullanıcıları tatmin noktasına oldukça yaklaşan bulut bilişim hizmetlerinin temel problemi hizmet sağlayıcı ve kullanıcı arasında güven mekanizmasının henüz yeterli olgunluk seviyesinde oluşturulamamış olmasıdır. Bu güven mekanizmasının oluşturulmasında ortak anlayış ve denetlenebilirlik sağlaması açısından standardların yayımlanması ve bu standartların rehberliğinde gereken hukuki düzenlemelerin hayata geçilmesine ihtiyaç vardır. Bu çalışmada, bulut bilişimin yayınlaşmasının önündeki en önemli engel olan güvenlik boyutuna dikkat çekilmekte ve Türkiye'de bulut bilişim konusunda devam etmekte olan standart çalışmaları hakkında bilgi verilmektedir. Bulut bilişim ve e-devlet hizmetlerinin bu standard çalışmalarına paralel geliştirilmesinin önemi vurgulanmaktadır.**

***Anahtar Kelimeler*— Bulut bilişimde güvenlik, bulut bilişim güvenlik standardları**

I. GİRİŞ

SAYISAL çağ olarak isimlendirilen 21nci yüzyılın ilk on yıllık döneminde, sayısal ortamların büyük bir hızla sosyalleşmesi gözlenirken, veri saklama ve hesaplama hizmetlerine donanım ve fiziksel mekândan bağımsız erişim sağlayan bulut bilişim uygulamaları da yaygınlaşmaktadır. Bilgisayar ağ altyapısında erişilen sürat ve yaygınlaşmaya paralel olarak, veri ve hizmetlerin ağ üzerinden kullanılması daha cazip hale gelmektedir. E-ticaret, e-bankacılık, e-devlet ve uzaktan eğitim gibi geniş kullanıcı kitlesine hitap eden hizmetler internet ağı üzerinde başarılı bir şekilde kullanılmaktadır. Bütün bu gelişmelerin yanında bulut bilişim yaklaşımı özellikle hizmet maliyetlerini düşürmesi ve yüksek erişilebilirlik özellikleri ile yeni fırsatlar yaratmaktadır. Yapılan stratejik değerlendirmeler, bulut bilişim uygulamalarının yaygınlaşacağını ve bu alanda ekonomik gelişmeler yaşanacağına işaret etmektedir. Dünya genelinde bu alandaki pazarın 2010 yılında 21,5 milyar dolar olduğu belirtilirken, 2015 yılı için bu rakamın 73 milyar dolara ulaşacağı öngörülmektedir [1]. AB ekonomisinde de bulut bilişimin önemli bir stratejik etken olması beklenmektedir [2].

Bulut bilişim konusunda yapılan inceleme ve araştırmalar güvenlik ve kişisel bilginin korunması boyutlarının bu teknolojinin yaygınlaşmasının önünde en önemli engelleri oluşturduğu konusunda hem fikirdir [3], [4], [5]. Bu engellerin aşılması için ise öngörülen çözüm yolu, alanda ortak standartların belirlenmesi ve hukuki düzenlemelerin yapılması olarak ortaya çıkmaktadır.

Varadi ve diğerlerinin [6] de belirttiği gibi, bilgi güvenliğinin sağlanması ve kişisel bilginin koruması konuları teknik çözümlerin yanında hukuksal düzenlemelerle de yakından ilgilidir. Mevcut hukuki düzenlemelerin ise devletlerin hâkim oldukları coğrafya ile sınırlanmış olması, bulut bilişimin doğasında var olan coğrafyadan bağımsız olma ve hizmet yerinin bilinmemesi prensipleri ile yan yana konduğunda problemi daha da karmaşık hale getirmektedir. Güvenin sağlanması ve kişiselliğin korunması problemleri bankacılık sisteminin kurulduğu yıllarda da ortaya çıkmış, ancak bu problemler devletlerin hukuki düzenlemeleri ile günümüzde aşılmıştır. Ne var ki, bankacılık konusundaki hukuki düzenlemeler devletlerarasında farklılık gösterebilmektedir. Geçerli olan düzenleme, bankacılık hizmetinin verildiği devlet sınırları ile belirlenmektedir. Bulut bilişim ise hizmetin coğrafyadan bağımsız olarak ve farklı devlet hâkimiyetlerinde bulunan sistemlerden alınmasını öngörmektedir. Bu tür bir hizmet sunumu teknik olarak mümkün olsa da hangi hukuki düzenlemeye tabi olacağı konusu halen tartışılmaktadır [7], [8].

Diğer taraftan birçok ülkede e-devlet uygulamaları ile kamu hizmetlerinin bir bulut içerisinde vatandaşa ulaştırılması ve böylece, bu hizmetlerin maliyetlerinin düşürülmesinin yanında, hizmet süratinin ve erişilebilirliğin artırılarak vatandaş memnuniyetinin yükseltilmesi amaçlanmaktadır. Bu amaçla Türkiye'de 2003 yılından itibaren Bilgi Toplumu Stratejisi yayınlanmış ve buna uygun bir eylem planı hazırlanarak uygulamaya geçilmiştir. Ancak özellikle kamu kurumlarının kendi sorumluluklarına verilen bilgi ve süreçleri, kurum dışına açmasında ortak standart ve hukuki düzenleme yetersizliği önemli bir engel oluşturmaktadır. Zira her kurum kendi sorumluluğundaki bilginin korunması ve hizmetlerin uygun şekilde

Manuscript received July 15, 2013.

Gökhan Şengül is with Computer Engineering Department, Atilim University, Gölbaşı, Ankara TURKEY (tel:+90 312 586 8826 e-posta:gsengul@atilim.edu.tr). Atilla Bostan is also with Computer Engineering Department, Atilim University, Gölbaşı, Ankara TURKEY (e-mail: abostan@atilim.edu.tr)

çalışmasından sorumlu ve yetkili iken, kurumsal sorumluluk alanında uygun düzenlemeler yapılmadan yetkinin başka otoritelere devrine karşı çıkmaktadır. Bu konuda yaşanmış olan ve bulut servis sağlayıcısından kaynaklanan hizmet aksaması ve veri kaybı olayları da kaygıları kuvvetlendirmektedir. Bulut hizmeti vermekte olan Intuit sitesi 15-16 Haziran 2010 tarihinde 24 saati açan bir süre zarfında hizmet verememiş, bu da birçok kullanıcı için mağduriyet oluşturmuştur [9]. En yeni olaylardan birisi de, bulut hizmet sunucusu Evernote'un Mart 2013 tarihinde 50 milyon kullanıcı parolasının saldırgan kişilerce değiştirildiğini açıklamasıdır [10]. Bütün bunlara rağmen bulut bilişimin vaat ettiği hizmet edinme ve işletmesindeki düşük maliyet ve hizmet sunumundaki esneklik, devlet bulutunun bir ön adımı olabilecek kamuda veri merkezlerinin birleştirilmesi [11] gibi bazı çalışmaların başlatılmasının önüne geçememektedir.

Bu çalışmada öncelikle bulut bilişim kavramı, hizmet modelleri, faydaları hakkında özet bilgi verilecek ve bulut bilişimim yaygınlaşmasının önündeki sorunlar listelenecektir. Daha sonra bulut bilişimin önde gelen sorunlarından olan güvenliğin sağlanmasında standartların önemi ve Türkiye'de sayısal güvenlik standardı çalışmaları anlatılacaktır. Sonuç bölümünde ise ülkemizdeki güvenlik standartları konusunda beklenen gelişmeler ışığında bulut bilişim ve e-devlet uygulamalarında gerçekleşebilecek açılımlar vurgulanacaktır.

II. BULUT BİLİŞİM

Bulut bilişim konusunda üzerinde uzlaşı sağlanan bir tanımlama henüz bulunmasa da; bu kavramı, erişim noktaları arasında ortak bilgi ve hizmet paylaşımını sağlayan platform olarak tanımlamak mümkündür. Tanından da anlaşılacağı üzere erişim noktaları arasında iletişimi, bilgi akışını sağlayabilmek için bir iletişim ağına ihtiyaç vardır ve bu ağ bulut bilişimi mümkün kılan en temel bileşendir. Bir başka bakış açısından bulut bilişim için veri ve hizmetlerin bir ağ üzerinden ve kullanıcılar arasında ortaklaşa kullanılmasıdır tanımı da yapılabilir. Aslında ağ üzerinden hesaplama, dağıtık hesaplama veya ağ üzerinde dağıtık veri saklama bilişim dünyasında uzun zamandan beri yapıla gelen uygulamalardır. Son zamanlarda, veri ağlarının yaygınlaşması, süratlerinin artması, erişim ve kullanım maliyetlerindeki düşüş ile sanal işlem ve sanal saklama alanlarındaki ilerlemeler, tüm bu özellikleri içeren hizmetlerin daha etkin ve düşük maliyetle üretilmesini mümkün kılmıştır. Artık kullanıcının fiziksel olarak kaynağını bilmediği hizmetleri kullanması veya yine fiziksel olarak makine ve ortamını bilmediği alanlarda verilerini saklaması mümkündür. Kullanıcı bakış açısından hesaplama hizmetleri ve veri saklama alanları fiziksel bir cihaza karşılık gelmeyen bir ortam (bulut) tarafından sağlanmaktadır.

Yukarıda bahsedilen karakteristikteki hizmetlerin İnternet gibi evrensel bir ağ üzerinde çalıştırılması ile mekândan ve donanımdan bağımsız erişim altyapısı sayesinde, hem hizmetlerin erişilebilirliği artmakta hem de daha geniş bir kullanıcı kitlesine hizmet vermek suretiyle kullanıcı başına düşen maliyetler azalmaktadır.

Günümüzde kullanılmakta olan bulut bilişim hizmetleri farklı bakış açılarından değişik sınıflandırmalar altında toplanabilmektedir. Aşağıda sırası ile bulut bilişimin farklı bakış açılarından sınıflandırmaları, bulut bilişimin faydaları ve sorunları sunulmuştur.

A. Bulut bilişim Sınıflandırmaları

1. *Verilen Hizmet Açısından Bulut Modelleri*

Bulut bilişim hizmetleri genellikle üç hizmet modeli ile sınıflandırılmaktadır. Hizmet sağlayıcılar bu modellerden herhangi birisini veya birkaç tanesini eş zamanlı sunabilmektedir. Bu hizmet modelleri ve özellikleri aşağıda özetlenmiştir.

i. Hizmet Olarak Yazılım (Software as a Service--SaaS).

Bu hizmet modelinde kullanıcı terminallerine yazılım yüklemesi yapılmadan, yazılımlar hizmet bulutu içerisindeki sunucular üzerinde çalıştırılır.

ii. Hizmet olarak platform (Platform as a Service-PaaS).

Kullanıcıya geliştirme ortamı gerekli tüm yazılım, donanım ve konfigürasyonları ile sağlanır. Kullanıcı bu ortamı, kullandığı terminalden ve mekândan bağımsız olarak kullanır.

iii. Hizmet olarak Altyapı (Infrastructure as a Service-IaaS)

Kaynak bulutu olarak da adlandırılır. Bilişim altyapı elemanı hizmetlerini bir bulut içerinde sunma esasına dayanır. Veri saklamak için disk alanı, ağ güvenliği için ateş-duvarı hizmetleri bu model için örneklerdir.

2. *Kullanım Biçimine Göre Bulut Modelleri*

Kullanım Biçimine göre bulutlar dört sınıfa ayrılmaktadır.

i. Genel Bulut.

Genele açık bir ağ üzerinden verilen bulut bilişim hizmetleridir.

ii. Özel Bulut.

Bir kurum, firma gibi belirli bir grup kullanıcı için verilen bulut hizmetleridir. Hizmetler kurumun, firmanın kendisi tarafından veya farklı bir kuruluş tarafından çalıştırılabilir.

iii. Melez Bulut.

Genel ve özel bulutun karışık ve eş zamanlı kullanımıdır. Belirli bir kurum, firma bazı hizmetleri genel buluttan alırken diğerlerini özel buluttan alabilir..

B. Bulut Bilişimin Faydaları

Bulut bilişim donanım, yazılım ve altyapının ortaklaşa kullanılmasını sağlaması nedeni ile bu maliyetlerin paylaşılmasını sağlamaktadır. Ayrıca sistem işletmesi, güvenliğin sağlanması ve yedekleme gibi bazı özel hizmetlerin de daha kaliteli yerine getirilmesine yardımcı olmaktadır. Servis model ve kullanım şeklinden bağımsız olarak bulut bilişimin faydaları;

i. Donanım ve yazılım maliyetlerinin azalması
ii. Uzaktan erişim kolaylığı
iii. Veri saklama maliyetlerinin veri miktarı ile orantılı olması.

olarak sıralanabilir. Bütün bunlara ek olarak, Avrupa Komisyonu 2012 yılı raporuna göre bulut bilişim sayesinde mobil çalışma %46, üretim %41 ve standartlaşma %35 artmıştır [12]..

C. Bulut Bilişimin Sorunları

Bulut bilişimin faydalarının yanında nispeten yeni bir

yaklaşım olması ve ülke sınırlarını aşan bir hizmet olması nedenleri ile halen bazı teknik ve hukuksal sorunları bulunmaktadır. Özellikle hukuksal sorunların bulut bilişimin yaygınlaşmasının önünde önemli engel oluşturduğu değerlendirilmektedir. Bulut bilişimin mevcut sorunları başlıklar halinde aşağıda listelenmiştir.

i. Uygulamaların yavaş çalışması
ii. Geniş bant ağ erişimine ihtiyaç duyması
iii. Uzaktan erişim güvenlik sorunları
iv. Hizmet ve/veya verinin nerede olduğunu bilmeme
v. Bulut hizmeti veren firmanın yeterliliğinin ve güvenirliliğinin bilinmemesi ve denetlenememesi
vi. Bulut hizmeti veren firmaların güvenlik, veri bütünlüğü ve erişim denetimi konularında sorumluluk üstelenmemeleri
vii. Bulut hizmeti veren firmaların hizmet sürekliliği konusunda taahhütte bulunamaması
viii. Buluttaki içeriğin mülkiyet hakkı ve kullanımı konusunda belirsizlik
ix. Sayısal deliller ve adli inceleme işlemleri, süreçleri konularındaki belirsizlikler.
x. Siber saldırılar için bulut alanlarının hedef haline gelmesi.

Yukarıdaki listede belirtilen ilk iki madde dışında kalan diğer maddelerin hepsi bulut hizmeti kullanıcısının hizmeti veren makamla olan güven ilişkisini doğrudan etkileyen hususlardır. İlk iki maddede belirtilen bulut sorunları halen alanda sorun olarak yer almakla beraber, günümüzde erişilen durum itibarı ile kullanıcı rahatsızlığı açısından çok ön planda olan konular değildir. Bir başka ifade ile bulut bilişimde en temel sorun, hizmet sağlayıcısı ve kullanıcısı arasındaki güven mekanizmasındaki eksiklikler ve bu alanda geçerli olacak hukuksal düzenlemelerin eksikliği olarak göze çarpmaktadır.

III. GÜVENLİĞİN SAĞLANMASINDA STANDARTLARIN ÖNEMİ

Herhangi bir ürünün, sürecin, sistemin ya da kişinin, önceden belirlenmiş kriterlere göre değerlendirilmesi ve söz konusu kriterlere uygunluğunun üçüncü taraflarca doğrulanması süreci belgelendirme olarak adlandırılmaktadır. Genellikle değerlendirme kriterleri, üzerinde tüm paydaşların katılımı ile belirlenir ve ulusal ve uluslararası standardizasyon kuruluşları tarafından standart olarak yayınlanır. Herhangi bir standardda ürünün belirli özelliklere göre sağlaması gereken kriterler yer alır. Örneğin bilgi teknolojileri cihazları ile ilgili bir standart, cihazın sağlaması gereken işlevselliğe odaklanırken bir başka standart aynı ürünün uyması gereken bilgi güvenliği prensiplerine odaklanabilir.

Türkiye'de standartların hazırlanması ve standartlara uygunluk sağlayan firma ve ürünlerin belgelendirilmesi görevi 132 sayılı kanunla Türk Standardları Enstitüsü'ne (TSE) verilmiştir. 1960 yılında kurulan TSE, o günden bu yana farklı alanlarda standart hazırlama faaliyetlerini sürdürmektedir. Bugün itibariyle TSE tarafından yayınlanmış olan yürürlükte 30000'den fazla standart bulunmaktadır. Uluslararası alanda ise standart hazırlama çalışmalarını yürüten farklı kuruluşlar bulunmaktadır. Uluslararası düzeyde standart hazırlama çalışmalarını yürüten en büyük kuruluş hiç kuşkusuz ki Uluslararası Standardizasyon Teşkilatı (ISO) 'dur. Uluslararası alanda standart hazırlama faaliyetinde bulunan bir diğer büyük kuruluş ise Uluslararası Elektroteknik Komisyonu (IEC)'dir. Türk Standardları Enstitüsü hem ISO'nun hem de IEC'nin üyesidir ve söz konusu kuruluşların standartlarını da Türk Standardı olarak kabul etmekte ve yayınlamaktadır. Türk Standardları Enstitüsü (TSE) ayrıca, 2011 yılında Avrupa Birliği (AB) standardizasyon kuruluşları olan Avrupa Standardizasyon Komitesi (CEN) ve Avrupa Elektroteknik Standardizasyon Komitesi (CENELEC)'ne de tam üye olmuştur. Türk Standardları Enstitüsü, hem ülkemiz ihtiyaçlarına yönelik standart hazırlama faaliyetlerine devam etmekte, hem de mevzuatlar gereği üyesi bulunduğu uluslararası standardizasyon kuruluşlarının standart hazırlama çalışmalarına katılmakta ve bu kuruluşlarca yayınlanan standartları Türk Standardı olarak kabul etmektedir.

Bilgi güvenliği konusundaki standartlara değinmeden önce söz konusu standartlara göre belgelendirme yapmanın öneminden bahsetmek gerekir. Bilgi güvenliği standartlarına uygunluğun sağlanması ve dolayısı ile belgelendirme yapılması, BT ürünleri ya da sistemlerinde en az bilgi güvenliği açığı ya da zafiyeti bulunduranların tespit edilmesi ve temini ile bilgi güvenliği konusundaki risklerin en aza indirgenmesini sağlayacaktır. Bu sayede gerek maddi gerekse de manevi kayıpların en aza indirilmesi mümkün olabilir.

Bilişim sektöründeki ürünler ve sistemler baz alındığında gerek uluslararası düzeyde gerekse de ulusal düzeyde birçok standardın bulunduğu görülebilir. Ancak söz konusu olan bilgi güvenliği olduğunda, ulusal ve uluslararası standartları iki temel grupta ve standart başlığı altında toplamak mümkündür: Sistem tabanlı standartlar (ISO/IEC 27001 grubu) ve ürün tabanlı standartlar (ISO/IEC 15408 grubu).

TS ISO/IEC 27001 [13], ilk olarak ISO tarafından 2005 yılında yayınlanmış, müteakibinde Türkçeye tercümesi yapılarak Türk standardı olarak TSE tarafından da yayınlanmış bir sistem tabanlı bilgi güvenliği standardıdır. Standard herhangi bir ürünün taşıması gereken güvenlik kriterlerini belirlemez. Bunun yerine BT ürünlerini kullanan bir sistemi ele alarak Bilgi Güvenliği politikası, risk analizi, iç denetimler, yönetim desteği ve yönetimin gözden geçirmesi gibi konuları ele alarak bir kuruluştaki bilgi varlıklarının korunmasına yönelik olarak sistemin gereksinimlerini belirler. ISO tarafından söz konusu standardı destekleyici diğer bir dizi standart da (ISO 27000, ISO 27002, ISO 27004, ISO 27005, ISO 27006, vb) yayınlanmıştır. Söz konusu standartlar yine TSE tarafından Türk standardı olarak kabul edilmiş ve yürürlüktedir.

Bunun yanında BT ürünlerinin taşıması gereken asgari güvenlik kriterlerini belirleyen ve belgelendirilmesini sağlayan ürün temelli bir standart olan ISO/IEC 15408 standardı bulunmaktadır [14]. Ortak kriterler olarak da bilinen ISO/IEC 15408 standardı ilk kez 2005 yılında yayınlanmış, 2009 yılında da revize edilmiştir. Ortak kriterler ISO 15408 -1,2,3 şeklinde üç bölümden oluşmaktadır ve belirli bir BT ürününe özgü olmayıp tüm ürünlere uygulanabilirdir. Standart EAL olarak adlandırılan ve 1'den başlayıp 7'ye kadar uzanan yedi güvenlik seviyesi belirlemektedir. Bu seviyelerden EAL-1 en düşük seviyeyi, EAL 7 ise en yüksek seviyeyi ifade eder. Genellikle yazılım ürünleri için EAL 4 ya da EAL 4+ en yaygın karşılaşılan

güvenlik seviyeleridir.

Bulut bilişim açısından güvenlik ele alındığında yukarıda bahsedilen standartlara göre belgelendirme yapmak mümkün olmakla birlikte bulut bilişimin doğası gereği bu belgelendirmelere hazırlanmak ve gerekli denetimleri gerçekleştirmek zordur. Bunun yanında güncel bir teknoloji olması itibariyle bulut bilişim alanında bilgi güvenliği kriterlerini belirlemek amacıyla henüz yayınlanmış özel bir standart da bulunmamaktadır. Ancak gerek sektördeki gerekse de bulut bilişimin hızla yaygınlaşması ve bu nedenle de bilgi güvenliği hususlarının irdelenmesi ihtiyaçları nedeniyle hem ISO bünyesinde hem de TSE bünyesinde standardizasyon çalışmalarına başlanmıştır.

ISO bünyesindeki çalışmalar incelendiğinde ISO/IEC 27017 [15], ISO/IEC 27018 [16] ve ISO/IEC 27036-4 [17] standartları konusunda çalışmalara başlandığı görülmektedir. Bu standart çalışmalarından ilki olan ISO/IEC 27017 çalışması, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardını temel alarak bulut bilişim hizmetleri için bilgi güvenliği kontrolleri için en iyi uygulama örneklerini, ISO/IEC 27018 çalışması halka açık bulut bilişim hizmetlerinde veri koruma kontrollerinin en iyi uygulama örneklerini ve ISO/IEC 27036-4 ise tedarikçi hizmetleri açısından bulut bilişim güvenliği kılavuzu sağlamayı hedeflemektedir. Her üç standart çalışması da incelendiğinde ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi tabanlı oldukları ve henüz standart hazırlama çalışmalarına yeni başlandığı ve standardların yayınlanmasının zaman alacağı görülmektedir. Ancak yine de bulut bilişim konusunda hizmet sağlayan firmaların bu standardizasyon çalışmalarının farkında olmaları ve ürün tasarımlarını bu standardlara göre planlamaları faydalı olacaktır.

IV. TÜRKİYE'DE BULUT BİLİŞİM KONUSUNDAKİ STANDARDİZASYON ÇALIŞMALARI

TSE bünyesinde 2013 yılı ilk çeyreğinde oluşturulmuş olan "Siber Güvenlik Özel Komitesi" tarafından, bulut bilişim altyapılarının güvenliğine ilişkin standartların belirlenmesi yönünde çalışmalara başlanmıştır. Çalışma kapsamında bulut bilişim alanındaki uluslararası kuruluşlar ile başta Amerika olmak üzere öncü ülkelerin özellikle bulut bilişim güvenliğine yönelik çalışmaları incelenecek ve Türkiye için standartlar belirlenecektir. Bulut bilişim hizmet sağlayıcıları ülkemizde sayıca az olmakla birlikte, çok sayıda firmanın kişisel verilerini barındırıyor olmaları sebebiyle kritik öneme sahiptir. Bu nedenle bulut bilişime yönelik güvenlik standartları önemli görülmekte ve bu alandaki çalışmaların bir an önce bitirilmesi yönünde çaba harcanmaktadır.

Bulut bilişim kullanımının dünyada ve Türkiye'de yaygınlaşmasının önünde en önemli engel hizmet sağlayıcı ve kullanıcı arasında yeterli seviyede bir güven mekanizmasının sağlanamamış olmasıdır. Gerek hizmet sağlayıcıların belirli sorumlulukları üstelenmemesi ve gerekse alandaki hukuksal düzenleme belirsizliği bu karşılıklı güvenin oluşturulmasını engellemektedir. Kullanıcılar hizmetleri bulut üzerinden alırken ilave güvenlik risklerini üstelenmek istememektedir. Bu riskler, bilginin ve verinin güvenliği boyutunda olabileceği gibi, hizmetin sağlanması ve erişilmesi konularında da olabilmektedir. Kullanıcı açısından kişisel veya kurumsal verinin kaybı, bozulması, erişilememesi veya kendi kontrolü dışında üçüncü şahıslarca kullanılmasının yanında aldığı hizmetin sürekliliği ve erişilebilirliği önemli güven parametreleridir. Hizmet sunucusu ve kullanıcısı arasından bu alanda yapılacak sağlıklı anlaşmalar için hizmet güvenlik standardlarının belirlenmiş olması ve bir garantör otoritenin varlığına ihtiyaç duyulmaktadır. Standartların hizmet güvenlik seviyesi ve içeriği konusunda ortak anlayışı ve denetlenebilirliği sağlaması, garantör otoritenin ise bu standart ve düzenlemelerin ihlali durumunda zarar gören tarafın korunmasını garanti altına alması beklenmektedir. Aslında bu iki boyut birbiri ile çok yakından ilgilidir. Zira alanda ortak anlayış ve tanımlama sağlanmadan denetlenebilirlik ve hukuki düzenleme yapmak imkânsızdır.

V. SONUÇ VE ÖNERİLER

Günümüzde oldukça yüksek hızlara ulaşmış olan sayısal iletişim ve bilgi işleme teknolojisi kaynakların, hizmetlerin ve verinin ortaklaşa kullanılmasını sağlayan ve bulut bilişim olarak adlandırılan hizmet platformlarının yaygın olarak kullanılmasına imkân tanımaktadır. Ancak teknolojik olarak uygulanabilir olan bu hizmetler, alandaki güven problemlerinden dolayı yeterince hızlı yaygınlaşamamakta ve geniş kullanıcı çevrelerince tercih edilmemektedir.

Bulut bilişim hizmetleri için geliştirilecek ulusal ve evrensel standartların hukuksal düzenlemeleri de mümkün kılması ve hizmet sağlayıcı ile kullanıcı arasında oluşturulacak güven mekanizması için temel oluşturması beklenmektedir. Türkiye'de ISO/IEC kapsamında geliştirilmekte olan 27017, 2718 ve 27036-4 standartları ile bulut bilişim hizmetleri ve bulutta bilgi güvenliği konularında düzenleme çalışmaları başlatılmıştır. Ancak yeni yayınlanacak bu standartların temel olarak ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'ne dayanacak olması hizmet ve ürünlerde temel niteliklerin neler olacağı konusunda belirleyici faktördür. Bulut bilişim hizmet sağlayıcılarının hizmetlerini bu öngörü dâhilinde yapılandırmaları onlara gelecekte avantaj sağlayacaktır. Ayrıca e-devlet çalışmalarında ulaşılması hedeflenen devlet-bulutu hizmetlerinin de bu standart öngörüsüne paralel geliştirilmesi uygun olacaktır.

Standart çalışmalarına benzer şekilde bulut bilişime özgü hukuksal alanın düzenlenmesi konusunda da ulusal ve uluslararası çalışmaların bir an önce başlatılması zaman kazandıracaktır.

Bulut bilişimin yaygınlaşması ve daha geniş kullanıcı kitlerine ulaşması ancak hizmet sağlayıcı ve kullanıcı arasında karşılıklı güven mekanizmasının oluşturulması ile sağlanabilecektir. Standartların tanımlanmasını ve hukuki düzenlemeleri takiben bulut hizmetlerine talebin daha da artması ve bu hizmetlerin yaygın olarak kullanılması beklenmektedir.

KAYNAKLAR

[1] Fox B. (2012), Cloud computing a "game-changer" for EU economy, Kroes says, 30 Haziran 2013 tarihinde "http://euobserver.com/news/117695" adresinden erişildi.

[2] Kroes, N. (2012), Cloud computing and data protection reform. 30 Haziran 2013 tarihinde http://blogs.ec.europa.eu/neelie-kroes/cloud-data-protection adresinden erişildi.

[3] Khatibi V, Khatibi E. (2012), Issues on Cloud Computing: A Systematic Review, International Conference on Computational Techniques and Mobile Computing (ICCTMC'2012) December 14-15, 2012 Singapore, pages 212-216Henkoğlu T., Külcü Ö. (2012), Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme, Bilgi Dünyası, 2013, 14 (1) 62-86

[4] Brodkin J, 2008, 'Gartner: Seven cloud-computing security risks', Infoworld, 30 Haziran 2013 tarinde http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 adresinden erişildi.

[5] Varadi, S., Kertesz, A. ve Parkin, M. (2012). The necessity of legally compliant data management in European cloud architectures. Computer Law & security Review, 577-586.

[6] Kroes, N. (2012), Why we need a sound Do-Not–Track standard for privacy online, 30 Haziran 2013 tarihinde http://blogs.ec.europa.eu/neelie-kroes/donottrack/ adresinden erişildi.

[7] Catteddu D., (2010), Cloud Computing: Benefits, Risks and Recommendations for Information Security, Web Application Security Communications in Computer and Information Science Volume 72, 2010, p 17

[8] Hachman M. (2013), Update: Intuit Sites Outage Strands Thousands of SMBs, PCMag.com, 30 Haziran 2013 tarihinde http://www.pcmag.com/article2/0,2817,2365179,00.asp adresinden erişilmiştir.

[9] Hernandez D. (2013), Evernote Hack Exposes User Data, Forces Extensive Password Resets, wired, 30 Haziran 2013 tarihinde http://www.wired.com/threatlevel/2013/03/evernote-hack-password-resets/ adresinden erişilmiştir.

[10] Veri Merkezleri ve Güvenliği Konferansı 2013, 30 Haziran 2013 tarihinde http://www.webhostingturkey.com/post/2013/03/19/Veri-Merkezleri-ve-Guvenligi-Konferans%C4%B1-2013.aspx adresinden erişilmiştir.

[11] European Comission (2012), Unleashing the Potential of Cloud Computing in Europe, 03 Temmuz 2013 tarihinde http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf adresinden erişilmiştir.

[12] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements

[13] ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

[14] ISO/IEC WD 27017 Information technology -- Security techniques -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

[15] ISO/IEC CD 27018 Code of practice for data protection controls for public cloud computing services

[16] ISO/IEC WD 27036-4 Information technology -- Information security for supplier relationships -- Part 4: Guidelines for security of Cloud servic