

Bulut Hesaplama Güvenliği: Genel Bir Bakış

İlker Korkmaz¹, Fatih Tekbacak²

¹ İzmir Ekonomi Üniversitesi, Bilgisayar Mühendisliği Bölümü, İzmir

² İzmir Yüksek Teknoloji Enstitüsü, Bilgisayar Mühendisliği Bölümü, İzmir
ilker.korkmaz@ieu.edu.tr, fatih.tekbacak@iyte.edu.tr

Özet: Günümüz gelişen teknolojileriyle birlikte adı sıkça duyulan bulut hesaplama, işletmelerin, altyapıyı ve fiziki ortamı düşünmeden, platform bağımsız olarak, hazır bilgi servislerini kullanması ve her an her yerden bilgiye erişim hizmetini alabilmesi için oluşturulmuş genel çözüm platformudur. Bulut hesaplama sistemlerinde, büyük bulut yapısı içindeki servis kullanıcıları, yani müşteriler, servis sağlayıcı olarak hizmet veren kuruluşların sunduğu uygulamaları, yazılımları ve donanımları isteğe bağlı kullanım mantığıyla kiralar. Kullanıcılar, sanallaştırma sayesinde soyutlanan kaynakların fiziksel durumunu görmeksizin kendilerine sunulan hizmetlerden yararlanır. Bu aşamada, güvenlik unsuru önem kazanmaktadır. Bu çalışma, öncelikle bulut hesaplama teknolojilerini ve kullanım alanlarını ele alıp güvenlik unsurunun bulut hesaplama üzerindeki önemini vurgulamaktadır. Ayrıca, bulut hesaplama kullanılan güvenlik teknolojilerini ve bulut hesaplama üzerindeki temel güvenlik gereksinimlerini aktararak, bulut hesaplama güvenliği sistemdeki 3 farklı aktörün (sistem, uygulama geliştirici, kullanıcı) bakış açılarından incelemektedir.

Anahtar Sözcükler: Bulut Hesaplama, Güvenlik, Sanallaştırma, Güvenlik Gereksinimleri.

Cloud Computing Security: An Overview

Abstract: As having frequently been heard about its name with the emerging technologies, cloud computing is the general solution platform built to provide the enterprises with the ubiquitous data access service, in a platform independent form, without thinking of the infrastructural and physical environment. In cloud computing systems, service users of the big cloud structure, the customers, rent the applications offered by the service provider enterprises via a logic of on-demand use of softwares and hardwares. Users use the services offered to themselves without being aware of any physical condition of the resources that are abstracted by virtualization. In this manner, the security issue gets importance. This study, firstly considering the cloud computing technologies and their application areas, emphasizes the importance of the security issue in cloud computing. Furthermore, explaining the security technologies and fundamental security requirements in cloud computing, examines the cloud computing security within the perspectives of 3 different actors (system, application developer, user) of the system.

Keywords: Cloud Computing, Security, Virtualization, Security Requirements.

1. Giriş

“United States National Institute of Standards and Technologies” (NIST) [1] tarafından yapılan tanıma göre, bulut hesaplama, dağıtık, kullanışlı ve ayarlanabilen hesaplama kaynaklarının içinde bulunduğu paylaşılabılır bir havuza yönelik taleplere cevap verecek olanakları sağlayan bir modeldir. Bulut hesaplama ile ağları, sunucuları, depolama birimlerini, uygulamaları ve servisleri içeren kaynaklar hızlı bir şekilde sunulabilmekte, yönetim için harcanan çabaya veya servis sağlayıcı etkileşimine en az seviyede ihtiyaç duyulmaktadır.

Bulut hesaplama mevcut kaynaklar, uzak veri merkezlerindeki donanımları ve sistem yazılımlarını içerir. Kaynaklar, internet üzerinden erişime imkân verilen servisler aracılığıyla, “kullandığın kadar öde” iş modeli üzerinden dinamik olarak yönetilebilmektedir [2].

Bulut sistemlerinde uygulama/yazılım geliştiricileri, gerçekledikleri proje uygulamalarını çeşitli servisler şeklinde bulut içinde hazır tutar. Kullanıcılar, dağıtık kaynaklar arasından istedikleri servisleri veya ürünleri

kendi çözümleri için kullanmak üzere kiralar. Kullanıcıların istekleri doğrultusunda kullandıkları kadar ödeme yaptıkları bu sistem “kazan-kazan” sistemi şeklinde sürdürülmektedir. Buluttan yararlanan kullanıcı şirketler, yani müşteriler, yüksek altyapı kurulum masraflarından arınmaktadır. Servis sağlayıcılar ise hazırladıkları servisleri bir kere bulut içine yerleştirip tüm kullanıcılara ayrı ayrı yüksek ek operasyon maliyeti üretmeden web uygulama sunucuları aracılığıyla tek bir servisten çok kullanıcının yararlanabileceği nitelikte sunmaktadır. Bu bağlamda, bulut hesaplama, yeni iş fırsatları için yüksek potansiyelli bir pazar imkânı doğurmuştur.

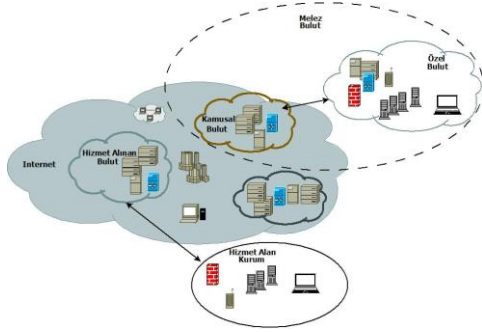
2. Bulut Hesaplama Ortamı

2.1 Bulut Teknolojileri

Şekil 1’de küresel internet içindeki genel bulut yapısı, kamusal, özel ve melez türleri açısından örnek olarak resmedilmiştir. Kurumlar, kendi özel bulut hesaplama

sistemini kurabileceği gibi, başka bir kamusal bulut hesaplama sisteminden hizmet alabilir ya da hem kendi özel bulut sistemlerinin hem de halka açık kamusal bulut sistemlerinin sunduğu hizmetlerden yararlanacak biçimde bir melez bulut yapısı oluşturabilir.

Uygulama ve yazılım geliştiricilerin, genel olarak yazılım geliştirme süreçlerini bulut mimari içinde kullanırken, eklentiler aracılığıyla genişletilebilecek tarzda, modüler bir yapıda ve çevik biçimde kodlama gerçekleştirmeye çalışmaları anlamlı olacaktır. Hızla gelişen bulut sistemlerinde servis uygulamalarının çabuk oluşturulması istenmektedir. Bu doğrultuda, bulut ortamlarında program geliştirme teknolojileri olarak, hazır kütüphaneler barındıran, bunlarla ilişkili uygulama programlama arayüzleri sunan ve bulut standartlarına yönelik çözümleri destekleyen yazılım teknolojileri tercih edilmektedir. Böylece, daha önceden farklı platformlarda program geliştirmiş olan uygulama geliştiriciler de bulut ortamlarına yönelik yazılımlar üretmeye çabuk adapte olabilir. Bu bağlamda, bulut teknolojileri kapsamında yazılım geliştiriciler arasında adı sıkça geçen, web uygulaması geliştirmek ve barındırmak üzere hizmet olarak platform (“Platform as a Service”, PaaS) şeklinde kullanılan teknolojilerin bazıları şöyle sıralanabilir: Google App Engine [3], Engine Yard [4], Force.com [5], Heroku [6], VMware [7], Amazon Web Services (AWS) [8], Windows Azure [9].



Şekil 1. Genel olarak bulut yapısı.

2.2 Bulut Uygulama Alanları

Dağıtık ortamda paylaşılan havuzdaki kaynaklar, sanallaştırma veya iş çizelgeleme ile birleştirilebilmektedir. Hizmet olarak altyapı (“Infrastructure as a Service”, IaaS) şeklinde görülebilen sanallaştırma, genellikle fiziksel kaynaklar gibi davranan ve yazılım bileşenleri tarafından gerçekleştirilen mantıksal kaynak kümelerinin oluşturulmasıdır. Böylece, kullanıcılar tüm bulut altyapısını fiziksel olarak algılamaya ihtiyaç duymadan kullandıkları uygulamalarla ilişkili sunucu servisleri ile etkileşimde olur [2].

Bulut mimarisinde, tüm uygulamalar sunucu cihazlar üzerinde konuşlanmaktadır. İstemci cihazlar, internet imkanı olduğu sürece, her an her yerden uygulamaya erişebilir. Ayrıca, istemciler, sunucular tarafından

sunulan web servisleri benzeri araçlarla dağıtık ortamdaki veri tabanlarında ve/veya veri merkezlerinde konuşlandırılan verilere de erişebilir. Dolayısıyla bulut hesaplamanın en temel uygulanma biçimi, müşterilere her an her yerden veriye erişim imkânı sağlanabilmesidir ki bu da her sektörün her alanı ile ilişkilendirilebilir. Ayrıca, günümüz kullanıcılarının gezgin iken de kesintisiz veri iletişimi alışkanlığının sürdürülebilmesi adına, bulut hesaplama ortamındaki güncel uygulama sunucuları son kullanıcıların akıllı telefonlarına, tablet bilgisayarlarına, dizüstü bilgisayarlarına ve elbette ki her türlü masaüstü bilgisayarlarına veriye erişim ve ilgili dağıtık uygulamalara bağlantı imkanı tanımaktadır. Son kullanıcıların bilhassa veri depolama hizmeti almak ve verilerine her an her yerden ulaşabilmek adına kullandıkları hizmet olarak yazılım (“Software as a Service”, SaaS) programlarına örnek olarak GoogleDrive [10], SkyDrive [11], Dropbox [12], box [13] verilebilir.

3. Bulut Hesaplama Güvenlik

3.1 Bulut Hesaplama Güvenlik Teknolojileri

Bulut hesaplama öne çıkan güvenlik unsurlarını sıralayabilmek adına, öncelikle, kullanılan güvenlik teknolojilerinin sunduğu servisleri araştırmak uygundur.

AWS ölçeklenebilir bir bulut hesaplama platformunu yüksek erişilebilirlik olanaklarıyla sunmaktadır [14]. AWS, servis sağlama sürecinde gerekli politikalar tanımlayarak kapsamlı bir kontrol ortamı sağlamaya çalışmaktadır. Bu noktada sertifikasyon amacıyla Federal Bilgi Güvenliği Yönetim Eylemi (FISMA), hükümet büro müşterileri ile uyumluluk, Sağlık Sigortası Taşınabilirlik ve Hesaplanabilirlik Eylemi (HIPAA) tarafından belirlenen sağlık alanında uygulama geliştiriciler için uyumluluk gibi güvenlik ve mahremiyet kuralları arz etmektedir. AWS’de kullanıcıların servisler üzerinde kimliklerinin belirlenmesi amacıyla, kullanıcı kimlikleri, parolalar ve Kerberos sistemi kullanılmaktadır.

Amazon Esnek Hesaplama Bulutu (EC2) [15], AWS’nin merkezi bölümünü oluşturmaktadır. Amazon EC2, bulut üzerinde tekrar boyutlandırılabilir hesaplama kapasitesi sağlayan bir web servisedir ve uygulama geliştiriciler için web bazlı hesaplamayı daha kolay hale getirebilmek için tasarlanmıştır. Bu amaçla, bir kullanıcı, örnek olarak oluşturduğu bir sanal makineyi Amazon Makine Görüntüsü üzerinde başlatabilir. Amazon EC2 güvenlik sistemleri, kullanıcının seçimi doğrultusunda çalışmakta olan örneklerini gruplara ayırma izni verir. Web servisleri arayüzünü kullanarak hangi grubun diğer hangi gruplarla iletişim içerisinde olduğu belirtilebilir ve internet üzerindeki hangi IP altağlarının bu gruplara erişebileceği tanımlanabilir. Böylece dinamik bir ortamda bahsedilen sanal makine örnekleri üzerinde erişim denetimi sağlanabilir.

Bulut hesaplamada sunulan diğer bazı güvenlik mekanizmalarına örnek olarak şunlar da sıralanabilir: Öncelikli kimlik yönetim desteği sunabilen Cyber-Ark [16] yazılım teknolojisi; güvenlik risk değerlendirmesi yapabilen ve bulut sunucularını iç ve dış saldırılara karşı korumak üzere kullanılabilen Cloud Passage [17] ateş duvarı; hesaplama iletişimini gözetleyebilen ve tehditleri daraltarak bütünüyle güvenlik sağlayıp verimliliği arttırmaya çalışan Lieberman Software [18] teknolojisi, Microsoft'un sağlam bulut için kullandığı Azure [9] ürünü, güvenlik de dahil genel bir bulut çözüm teknolojisi olarak Google App Engine [3].

3.2 Bulut Güvenliğinde Öne Çıkan Kavramlar

Bulut hesaplamasının birçok avantajı bulunmasının yanı sıra servislerde karşılaşılan bazı olası sorunlar göze çarpmaktadır. Bu sorunların başlıcaları, yerel veya bölgesel düzenlemelere uyumlu olma, erişim yetkisine sahip olunmayan alanlarda onay alınması gerekliliği, denetim açısından bazı ek karmaşıklıklar getirmesi, bulutun doğasına uygun olarak onarım ihtiyacı ve bulut servislerinde algılanabilecek güven eksiklikleri olarak sayılabilir.

Bulut bakış açısıyla lokasyonu ele alırsak, bilginin farklı noktalarda bulunabileceği bir sistemden bahsedildiği görülmektedir. Farklı noktalarda bulunan bilgi değişik bileşenler tarafından yönetilebilmekte, farklı coğrafi konumlarda bulunan sunucular üzerinde depolanmaktadır. Dolayısıyla veri ile ilgili uyumluluk gereksinimleri için küresel yasalara göre uzlaşmak zor olabilir ve bu durumda veriye sahip olma kısıtları, sektöre bağlı kısıtlar, ulusal veya eyalet bazındaki kısıtlar göz önüne alınmaktadır.

Küreselleşmenin hakim olduğu günümüzde, mahremiyet için geleneksel çatıların sunduğu yaklaşımlar tekrar gözden geçirilmektedir. Bağlam, farklı veriler üzerinde değişik mahremiyet, güvenlik ve gizlilik gereksinimleri doğmasında önemli bir argümandır. Bulut servisi eğer kişisel bilgileri ele almaktaysa mahremiyet hesaba katılmalıdır. Bulut servisleri halka ait bilgiyi işliyorsa düşük bir mahremiyet tehdidi öngörülebilir. Buna karşın, kişinin bulunduğu yere, tercihlere, sosyal ağlara ve bu gibi dinamik bilgilere göre kişiselleştirilen bulut servisleri için yüksek bir mahremiyet tehdidi öngörülebilir. Kişisel bilgilerin yanı sıra kurumsal bilgilerin ve ticari surların da ağ üzerinde paylaşımı dikkate alındığında gizlilik de önemsenmelidir.

Güvenilir bir bulut hesaplama sistemi, bilgiyi yetkisiz erişime karşı korumak, kimlik doğrulama sağlamak, çalınma veya kaybolmaya maruz kalabilecek cihazlar üzerinde duran hassas veriyi koruma amacıyla şifrelemek ve donanım/yazılım mekanizmaları ile uyumluluk sağlamak gibi güvenlik mekanizmaları sunmakla yükümlüdür [19]. Güvenilir Hesaplama Tabanı ("Trusted Computing Base", TCB), bilgisayar sistemi içindeki koruma mekanizmalarının bileşimidir; bir güvenlik politikasını yerine getirerek donanım,

yazılım ve gömülü aygıt yazılımının güvenilirliğini sağlar. TCB bileşenleri, bulut hesaplama sisteminin güvenlik politikasını yürütmekle yükümlüdür. Güvenilir Platform Modülü ("Trusted Platform Module", TPM), hesaplama için donanım tabanlı güven sağlayan bir standarttır. TPM, bilgisayar içerisine üretim esnasında eklenen bir bileşen de olabilmektedir. Bilgisayar üzerinde bulunan bir donanım elemanı olması vasıtasıyla kullanıcı ile birlikte cihazın da kimlik doğrulamasının yapılması için kullanılır.

Bulut hesaplama sağlayıcılarının birçoğu, güvenli bir bağlantı üzerinden kimlik doğrulama ve güvenli veri transferi gerçekleştirmesine rağmen, verinin şifreli saklanmasıyla ilgilenmemektedir. Dolayısıyla hassas verinin bulut üzerinde şifreli olarak bulunması kullanıcı tarafına bırakılan bir görev olarak görülebilir. Bulut hesaplama güvenliği, bulut içindeki kullanıcıların ve servis sunucularının verilerinin/uygulamalarının güvenliği, bulut hesaplama ile ilişkili kullanılan altyapının güvenliği için kullanılan yöntemler, kurallar ve teknolojiler ile ilişkilidir. Bulut güvenliğini sağlamaya yönelik gereksinimler, bulut altyapısında varsayılan olarak tanımlanmış sistem güvenliği mekanizmaları, kullanıcıların ve servis sağlayıcıların aralarındaki sözleşmeleri doğrultusunda anlaşılan veri erişimi kontrol mekanizmaları, servis seviyesinde erişim anlaşmaları, ayrıca kullanılan servisin sunduğu ek güvenlik işlevleri ile birlikte sağlanır. Bu kapsamda, bulut güvenliği gereksinimlerinin başlıcaları veri gizliliği, veri bütünlüğü, kimlik doğrulama olup bunların yanı sıra kimlik yönetimi, fiziksel ve kişisel güvenlik, erişilebilirlik, uygulama servisinin güvenliği, mahremiyet ve kanuna uygun unsurlar ek olarak öne çıkmaktadır [20].

3.3 Bulut Hesaplama Güvenliğine Farklı Açılardan Bakış

Bu kısımda bulut hesaplama sisteminde rol üstlenen bileşenlerin bulut hesaplama güvenliğine bakış açıları ele alınacaktır. Bu bağlamda, bulut yapılarındaki kullanım senaryolarında görev alan birimler, bulut mimarisi, BT yöneticisi, sistem yöneticisi, altyapı ve servis sağlayıcı, üçüncü parti güvenlik danışmanı, servis geliştirici, hizmet satıcı ve son kullanıcı gibi çeşitlendirilebilir. Ancak, bu çalışmada birimlerin 3 temel eylemci figürü üzerinde ele alınması planlanmıştır: sistem, uygulama geliştirici ve kullanıcı. Şekil 2'de, bu 3 temel bileşen, altyapı ve fiziksel destek bakımından bir bütün olarak kullanılan bulut sistemi, BT yöneticiliği, servis sunumu, danışmanlık, hizmet satışı, uygulama ve yazılım geliştirme bakımından aynı tarafta görülebilen bütün birimleri temsil etmesi adına uygulama geliştirici, hizmet alan kurumları ya da son kullanıcıları temsil etmesi adına kullanıcı ifadeleriyle gösterilmiştir. Şekil 2, bulut hesaplama sisteminin içinde yer alan bu temel birimlerin bulut hesaplama güvenliğine kendi

açılardan baktıkları durumda etkileşim içinde oldukları eylemleri ve dolayısıyla buluttaki kendileriyle ilişkili güvenlik görüş açılarını aktarmaktadır.

Şekil 2’de bulut sisteminde farklı kullanıcıların perspektifinden görülen öncelikli güvenlik unsurları ele alınmıştır; elbette ki sisteme ilgili birim tarafından bakıldığında bakış açısına girdiği düşünülen güvenlikle ilişkili özellikler daha da artırılabilir. Şekil 2’de, ilgili kesikli çizgilerin açısında kalan güvenlik unsurları belirtilirken en geniş açının sistem tarafında olduğu da resmedilmek istenmiştir. Her ne kadar en dar açıya sahip olan son kullanıcı güvenlikle ilişkili en az unsur içinde yer alıyormuş gibi görünse de kişisel olarak güvenlikten en fazla manevi zararı görebilecek olan da yine odur.

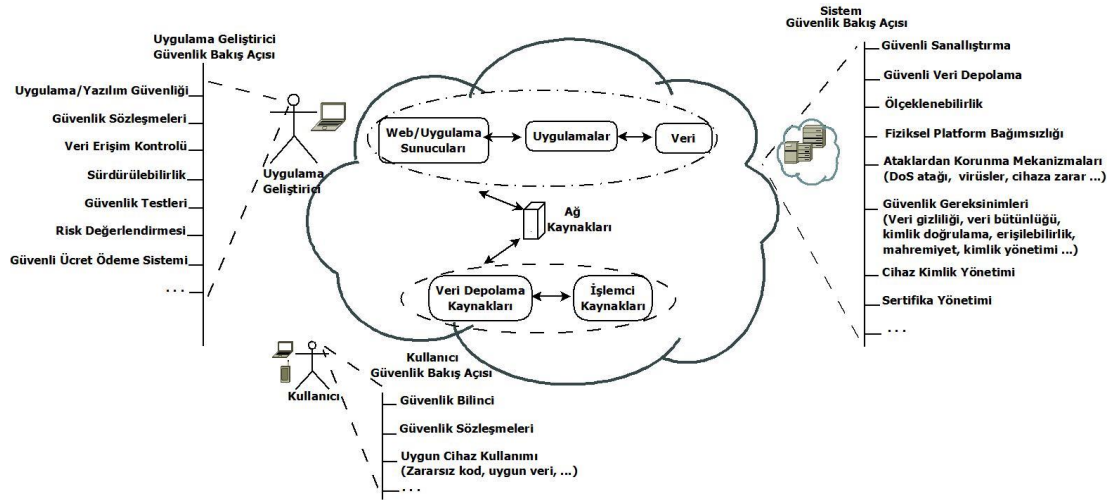
Sistem bakış açısından güvenlik:

Sistem her bileşenini güvenli biçimde yönetmek ister ve bileşenlerine zarar gelmesini istemez. Dağıtık ortamdaki tüm kaynakları korumaya çalışan sistem, servislerini uygulama sunucularında barındırır ve sistem tasarımcılarının veya uygulama geliştiricilerinin bu web servisleri aracılığıyla son kullanıcılara yönelik ek uygulama yazmalarını da destekler. Bu yolda güvenlik unsuru sistemin ayrılmaz bir parçası niteliğinde olmalıdır.

Özel, kamusal veya melez tipte oluşuna göre güvenlik gereksinimlerinin değişebileceği bulut sistemi, altyapısal bir güvenlik desteği sunmak yükümlülüğündedir. Sistemin güvenlik bakış açısında öncelikli görülen unsurlardan birisi güvenli sanallaştırma. Farklı sistem bileşenlerini ortamdaki son kullanıcılara platformdan bağımsız bir büyük veri merkezi ve içeriğindeki erişilebilir kaynaklar halinde sunmak üzere gerçekleştirilen yapılanmanın ağ güvenliği açısından dikkatle ve uygun konfigürasyonlarla düzenlenmesi ihtiyaçtır.

Çeşitli işlemci merkezleri veya son kullanıcı tarafından erişim için veri depolama merkezlerinde saklanan verilerin fiziksel güvenliği yine önemli ihtiyaçlardır. Ayrıca, sistemde güvenlik hizmetinin ölçeklenebilir olması beklenmektedir; dolayısıyla fiziksel kaynaklar, sunulan servisler, hizmet sağlayıcılar ve hizmet alıcılar arttıkça yani sistem bileşenleri çoğaldıkça güvenlik seviyesinin düşmemesi sağlanmalıdır.

Sistemin, ağ kaynaklarına yönelik saldırılara karşı korunma mekanizmalarıyla donatılmış olması öncelikli bir başka yükümlülük olarak görülebilir. Bulut hesaplama yapısına yönelik hizmet engelleme (“denial of service”, DoS) saldırıları, virüs yayma, fiziksel zarar verme ve ağa veya iletişime yönelik olası başka saldırılara karşı savunma mekanizmaları bulunması ihtiyaçtır.



Şekil 2. Bulut hesaplama ortamında farklı güvenlik bakış açıları.

Sistemin en temel güvenlik gereksinimleri açısından veri gizliliği, veri bütünlüğü ve kimlik doğrulama sunabilmesi istenir. Ayrıca, veriye her an her yerden erişilebilirlik, kişisel verilere yönelik mahremiyet hakkı ve kimlik yönetimi gibi gereksinimler de desteklenebilmelidir.

Sistem perspektifinden bulut hesaplama güvenliğiyle ilişkili görülebilen unsurlar daha da arttırılabilir. Sisteme katılan cihazlara kimlik numarası benzeri özellik atanması ve dolayısıyla kurumsal donanımlara yönelik kimlik yönetim desteği sunulabilmesi, ayrıca üçüncü parti güvenlik sertifikasyon hizmetleri için kriptografik anahtar oluşturma ve dağıtma sisteminin desteklenmesi ve dolayısıyla sertifika yönetiminin sağlanabilmesi bunlara örnektir.

Uygulama geliştirici bakış açısından güvenlik:

Uygulama geliştirici güvenlik bakış açısına göre, bulut üzerindeki uygulama/yazılım, kullanıcıların ihtiyaç duyduğu görevleri gerçekleştirirken gerekli ek güvenlik kıstaslarını da sağlar. Bu noktada, kullanılan yazılımlar izlenerek, oluşabilecek güvenlik tehditlerinden de korunmaya çalışılır.

Güvenlik sözleşmeleri, yazılım lisanslarındaki özellikleri andırmakla beraber dış kaynak kullanma kontratları gibi kullanılacak altyapıdaki yazılımdan başka donanımsal ve veriye özgü maddeleri de içerebilmektedir. Güvenlik ve uyumluluğun ön planda olduğu kontratlar, bölge bazında uygulanabilir kanunlar da göz önüne alınarak oluşturulmaktadır. Hizmet seviyesi anlaşma (“*Service Level Agreement*”, SLA) maddeleri baz alındığında altın, gümüş, bronz ve platin [21] gibi servis kullanım olanakları kategorize edilmekte, kontratlar buna göre düzenlenmektedir. Örnek olarak, “Microsoft SQL Azure Service Level Agreement” [22] bilgileri incelenirse, zamana bağlı (aylık, yıllık vs.) kontrat düzenlemeleri de görülecektir.

Bulut hesaplama ortamında veri erişim kontrolü için geliştiriciler, kullanıcılara sağladığı verinin güvenilirliği için denetim politikaları tanımlar. Bu noktada, hem servis sağlayıcıları hem de kullanıcılar tarafından meydana gelebilecek gizlilik, bütünlük ve güvenilirlik ile ilgili suçlamaların ortadan kaldırılmasına çalışılmaktadır. Bu amaçla ilgili erişim yetkisine sahip olmayan kişilerin veya kurumların, okumak, yazmak veya güncellemek istedikleri ilgili verilere, çalıştırmak istedikleri ilgili uygulamalara erişimleri kısıtlanmaktadır. Ayrıca veri veya uygulamanın silinmesi aşamasında ilgili kaynağın sürekli olarak başkaları tarafından erişilemeyecek şekilde silinmiş olması gibi durumların da kontrolünün sağlanması önemlidir.

Sürdürülebilirlik amacıyla yedekleme ve kurtarma kontrollerinin devamlılığının sağlanması gerekmektedir. Çoğu güvenlik ihlallerinin veri yedeklemesine dayalı olduğu düşünüldüğünde veri yedeklemesi üzerinde fiziksel ve mantıksal kontrollerin yapılmasının önemi anlaşılmaktadır. Bu

noktada özellikle fiziksel olarak yedeklenmiş verilerin hangi mekanizmalar yardımıyla yaşam döngüsünün devam ettirileceğinin üzerinde durulması önemli bir husus olarak göze çarpmaktadır.

Bulut üzerinde güvenlik testleri yapılırken, uygulama geliştiricinin bulut çözümünü kendi şirketinden veya diğer bir bulut sağlayıcısından aldığından bağımsız olarak test senaryoları geliştirmesi öngörülmektedir. Uygulamalar üzerinde yapılacak testlerin uygulamanın sınırları ile belirlenmesi gerekmele beraber bulut sınırlarının da önemsenebileceği güvenlik testleri yapılması düşünüldüğünde ağ altyapısının hesaba katıldığı durumlar meydana gelebilmektedir. Dolayısıyla beyaz-kutu veya kara-kutu test stratejilerinden hangisine uygun testler geliştirileceği uygulamaya ve bulutun altyapısına göre değişebilmektedir.

Risk değerlendirmesi, uygulama geliştiricilerin, ayrıcalıklı kullanıcı erişimi, verinin bulunduğu konum, verinin değerliliğine göre ayrımı, veri kurtarma, uygunsuz aktivitelerin araştırılması, uzun dönemde veri yaşayabilirliği gibi noktalarda uygun çözüm getirebilmek amacıyla analiz yaptıkları bir alandır.

Uygulama geliştiricinin de sunabileceği ek bir ihtiyaç olarak görülen güvenli ücret ödeme sistemi ise, kullanıcıların “kullandığın kadar öde” modeline uygun yaptığı ücret ödemelerinde kredi kartı bilgileri gibi hassas bilgilerinin korunmasına olanak sağlandığı bir tasarımla oluşturulmalıdır.

Kullanıcı bakış açısından güvenlik:

Şekil 2’de son kullanıcının güvenlik bakış açısı dar gösterilmiştir, çünkü kullanıcılar genel olarak güvenlik detaylarını önemsememektedir. Buluttan yararlanan son kullanıcı arka tarafı pek bilmez ve görmek de istemez, kendisine altyapı açısından güvenli bir sistem ve servis açısından güvenilir bir uygulama/yazılım sunulmasını ister.

Kullanıcıya düşen en önemli görev güvenlik bilincine vakıf olmaktır. Kullanıcı, sadece verilerine veya kendi mahremiyetine zarar vermemek adına değil aynı zamanda sisteme de olası tehdit sunmamak adına zararlı uygulamaları kullanmaktan kaçınmalı ve kendisi için verimli olabilecek güvenlik sözleşmelerini ele alıp bunlara uygun hareket etmeye çalışmalıdır. Sisteme erişim için kullandığı cihazların zararlı kod barındırmadığını takip etmesi de anlamlı olacaktır.

4. Sonuç ve Öneriler

Bu çalışmada, bulut hesaplama mimarilerinden, bulut hesaplama uygulama alanlarından ve bulut sistemlerinde kullanılan güvenlik teknolojilerinden bahsedilip bulut hesaplamada güvenlik gereksinimlerine değinilmiştir. Özel, kamusal veya melez biçiminde farklı tipteki ve farklı ölçekteki bulut yapılarının farklı güvenlik gereksinimlerine ihtiyaç duyabildiği ve tüm bulut yapıları için altyapısal mekanizmalarla desteklenmesi beklenen veri gizliliği,

bütünlük, kimlik doğrulama gibi temel gereksinimlerin yanı sıra erişilebilirlik, mahremiyet, kimlik yönetimi gibi bazı ek güvenlik unsurları vurgulanmıştır. Ayrıca, bulut sisteminin başlıca bileşenleri ve aktörleri olarak, sistemin kendi yapısı, sistemdeki uygulama geliştirici ve sistemdeki son kullanıcı tarafından farklı bakış açılarıyla bulut hesaplamada güvenlik unsurları değerlendirilmiştir.

Gelecek çalışmalara yönelik olarak, temsili bir bulut hesaplama sisteminde verilere ve ağa yönelik atak senaryoları hazırlanması, bu saldırılara karşı savunma mekanizmaları olarak kullanılabilen güvenlik gereksinimlerinin tasarlanması, bu senaryo bazlı sistemin yazılım süreçlerinin gerçekleştirilmesiyle uygulama testlerinin yapılması önerilmektedir.

5. Kaynaklar

[1] Mell, P. and Grance, T., "The NIST Definition of Cloud Computing". National Institute of Standards and Technology, Information Technology Laboratory. NIST SP 800-145. <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf> (2009).

[2] Pearson, S., "Privacy, Security and Trust in Cloud Computing". HP Laboratories. HPL-2012-80R1 (2012).

[3] Google App Engine, <https://developers.google.com/appengine/>

[4] Engine Yard, <http://www.engineyard.com/>

[5] Force.com, <http://www.force.com/>

[6] Heroku, <http://www.heroku.com/>

[7] VMware, <http://www.vmware.com/>

[8] Amazon Web Services, <http://aws.amazon.com/>

[9] Windows Azure, <http://www.windowsazure.com/>

[10] GoogleDrive, <https://drive.google.com/>

[11] SkyDrive, <https://skydrive.live.com/>

[12] Dropbox, <https://www.dropbox.com/>

[13] box, <https://www.box.com/>

[14] White Paper, "Amazon Web Services: Overview of Security Processes", Amazon Web Services (AWS), May 2011.

[15] Amazon Elastic Compute Cloud (EC2), <http://aws.amazon.com/ec2/>

[16] Cyber-Ark, <http://www.cyber-ark.com/>

[17] Cloud Passage, <http://www.cloudpassage.com/>

[18] Lieberman Software, <http://www.liebssoft.com/>

[19] Krutz, R. L. and Vines, R., D., "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley (2010).

[20] http://en.wikipedia.org/wiki/Cloud_computing_security

[21] Korn, A., Peltz, C., Mowbray, M., "A Service Level Management Authority in the Cloud". HP Laboratories. HPL-2009-79 (2009).

[22] Microsoft SQL Azure Service Level Agreement, <http://download.microsoft.com/download/B/0/9/B09851E2-6177-4A62-83AB-3B591659CE1E/SQL%20Azure/SQL%20Azure%20S LA-English.doc>