**Bulut Sistem Güvenliği, Saldırılar ve Saldırılardan Korunmak için Geliştirilen Yöntemler**

**Gül Deliorman, Özgü Can, Emine Sezer, Okan Bursa**

Ege Üniversitesi, Bilgisayar Mühendisliği Bölümü, Bornova-İzmir gul.deliorman@gmail.com,{ozgu.can, emine.sezer, okan.bursa}@ege.edu.tr

**Özet:** Bulut bilişimin gün geçtikçe yaygınlaşan kullanımı ile kişilerin günlük ve iş yaşamlarında olumlu değişiklikler meydana gelmiştir. Bulut sistem kullanımının artışıyla birlikte, bulut sistemler üzerindeki güvenlik de üzerinde durulan önemli maddelerden biri haline gelmiştir. Bulut sistemlerin yapısı gereği, çok kullanıcılı sistemlerin ve erişim kontrol düzeneklerinin yönetiminin zor olması, bazı güvenlik açıklarını doğurmaktadır. Bu çalışma kapsamında; bulut mimariler, bulut mimariler üzerindeki güvenlik riskleri ve açıkları, bulut saldırıları ve bulut saldırılarından korunmak için geliştirilen yaklaşımlar hakkında yapılan araştırmalar yer almaktadır.

**Anahtar Sözcükler:** Bulut Bilişim, Sistem ve Bilgi Güvenliği, Gizlilik, Saldırılar.

# Cloud System Security, Attacks and Improved Methods to Prevent Attacks

**Abstract:** Positive changes in people’s daily and work life have occured due to the expanding use of cloud computing. Cloud system security has become one of the most important substance with the increased use of cloud systems. Due to the nature of cloud systems, the difficulty of managing multi-user systems and access control mechanisms poses some security vulnerabilities. In this study; cloud architectures, security risks and vulnerabilities in the cloud architecture, attacks and improved methods to prevent attacks on cloud are being examined.

**Keywords:** Cloud Computing, System and Information Security, Privacy, Attacks.

# 1. Giriş

Telekomünikasyon endüstrisi, internetin ve mobil servislerin kullanımının yaygınlaşması ile gelişmiştir. Günümüzde, mobil servisler bulut ortamları tarafından desteklenmekte, bu da katma değer hizmetlerinin artması için büyük bir fırsat olarak görülmektedir. Telekomünikasyon endüstrisi, bulut bilişim çözümlerini kendi çözümleri ile birleştirmeye başlamıştır. Ericsson, kendi bulut ortamını yaratmış ve telekomünikasyon servis sağlayıcılarına bulut ortamları üzerinden hizmet vermeye başlamıştır [1]. Bulut bilişim, internet üzerinden hizmet veren bir teknolojidir. Bulut teknolojisi, yeni altyapıya ihtiyaç duymadan kapasitenin dinamik olarak genişletilebilmesi, yeni yazılım lisanslarına gerek olmaması ve yeni personeli eğitme gereksinimi olmaması nedeniyle maliyetleri oldukça azaltmakta; esnek ve ölçülebilir olduğu için de kullanıcılar tarafından tercih edilmektedir

[2].

İşletmelerin yanı sıra bireysel olarak da mobil aygıtlar aracılığı ile bulut sıklıkla kullanılmaktadır. Birçok kişi, mobil telefonları aracılığı ile internete bağlanıp, bulut uygulamalarını kullanmaktadır. Sağlık, eğlence, oyunlar, seyahatler, sosyal ağlar gibi birçok kategoride uygulamalar yazılmaktadır. Bulut bilişim, bilişim teknolojileri içerisinde önemli bir mimari sunmaktadır. Günümüzde gittikçe yaygınlaşan bulut kullanımı devrimsel doğasından dolayı, birçok güvenlik ve gizlilik risklerini de beraberinde getirmektedir [3]. Bulut üzerinde kiralanan yerler, bilginin önem seviyesine göre çeşitli yasal yükümlülükleri de beraberinde getirmektedir. Örneğin birçok Avrupa ülkesinde, bu tarz gizli bilgilerin bulunduğu sunucuların ülke dışına çıkışının olmaması gerekmekte ve bu durum yasalarla korunmaktadır [2].

Gizlilik, kültürden kültüre değişebilen öznel bir kavramdır. Bilgi teknolojilerindeki gizlilik; kişinin kendi haklarına karar verebilmesi, ne zaman ve nasıl bilgiye erişmek istediğini, kişinin kendisinin belirleyebilmesi anlamına gelmektedir [1]. Bu çalışmada, bulut bilişim mimarisi, bulut mimarisi üzerindeki güvenlik riskleri, bulut sistemler üzerine yapılabilecek saldırılar ve bu saldırıları önleme yöntemlerinden bahsedilmektedir. Bu çalışmanın içeriği şu şekildedir: ikinci kısımda bulut mimarisi güvenliği açıklanmakta, üçüncü kısımda riskler tanımlanmakta, dördüncü kısımda bulut sistemlerine yönelik saldırılar anlatılmakta, beşinci kısımda saldırıdan korunmak için gereken önlemler ve son olarak da sonuçlar sunulmaktadır.

# 2. Bulut Mimarisi Güvenliği

Bulut bilişim ortamları çoklu alanlı ortamlardır ve içerdiği her alt alan kendine göre farklı güvenlik, gizlilik ve güvenilirlik gereksinimlerine sahiptir. Birbirleriyle iletişim halinde olan alt birimlerde, bulut içerisindeki servis tabanlı mimari kullanımından faydalanılarak; güvenlik, gizlilik ve güvenilirlik gereksinimlerinin entegrasyonu kolaylıkla sağlanabilmektedir [4]. Bulut sistemler üzerindeki güvenlik, sistem üzerindeki rollere göre farklı gereksinimlere sahip olabilir. Bu amaçla, bu bölümde bulut mimarisi güvenliği sırası ile sistem, uygulama geliştirici ve kullanıcı bakış açılarından değerlendirilmektedir.

## 2.1 Sistem Bakış Açısından Güvenlik

Sistem, her bileşenini güvenli biçimde yönetmek istemektedir. Dağıtık ortamdaki tüm kaynakları korumaya çalışan sistemler, servislerini uygulama sunucularında barındırmakta ve sistem tasarımcılarının veya uygulama geliştiricilerin bu web servisleri aracılığıyla son kullanıcılara yönelik ek uygulama yazmalarını desteklemektedir. Bu nedenle; güvenlik, sistemin ayrılmaz bir parçası olarak nitelendirilmektedir. Ayrıca, sistemde güvenlik hizmetinin ölçeklenebilir olması beklenmektedir. Bu nedenle; fiziksel kaynaklar, sunulan servisler, hizmet sağlayıcılar, hizmet alıcılar arttıkça ve sistem bileşenleri çoğaldıkça güvenlik seviyesinin düşmemesi sağlanmalıdır [5].

**2.2 Uygulama Geliştirici Bakış**

# Açısından Güvenlik

Bulut üzerindeki uygulama, kullanıcıların ihtiyaç duyduğu görevleri gerçekleştirirken gerekli ek güvenlik gereksinimlerini de sağlamalıdır. Uygulamada yapılacak bir değişiklik, yazılım yaşam döngüsüne (software development lifecycle) etki etmektedir [6]. Özellikle; PaaS üzerinde sıklıkla güncellemeler yapılıp yeni sürümler geldiğinden dolayı, uygulamaların da bu sürümlere kolaylıkla uyarlanabilir olmalıdır. Bu nedenle, yazılımların esnek olması sayesinde bilgi güvenliği

artırılabilmektedir [6]. Güvenlik sözleşmeleri, yazılım lisanslarındaki özelliklere benzemekte ve 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) maddeleri baz alındığında altın, gümüş, bronz ve platin gibi servis kullanım olanakları sınıflandırılmakta, kontratlar buna göre düzenlenmektedir [7]. Örneğin, Microsoft SQL Azure Service Level Agreement [8] bilgileri incelendiğinde, zamana bağlı (aylık, yıllık vs.) kontrat düzenlemeleri de görülebilmektedir [5].

Sürdürülebilirlik amacıyla yedekleme ve kurtarma kontrollerinin devamlılığının da 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 düzenekler yardımıyla yaşam döngüsünün devam ettirileceğinin üzerinde durulması önemli bir husus olarak göze çarpmaktadır [5].

## 2.3 Kullanıcı Bakış Açısından Güvenlik

Kullanıcılar, verilerinin kendi kontrolleri dışındaki bir ortamda tutulmasından ve kendi kontrol edemedikleri bir zaman dilimi içerisinde işlenmesinden endişe duymaktadırlar. 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 etmelidir.

# 3. Bulut Mimariler Üzerindeki Güvenlik Riskleri

Bulut bilişimin mimari tasarımı ve karakteristiği sayesinde, güvenlik konusunda güvenliğin merkezileştirilmesi, veri ve süreç bölünmesinin sağlanması gibi birçok avantajı olmasına rağmen; bazı sorunlar da bulunmaktadır [9]. Bu sorunlar; yerel veya bölgesel düzenlemelere uyumlu olma, erişim yetkisine sahip olunmayan alanlarda onay alınması, denetim açısından ek karmaşıklıklar getirmesi ve bulut servislerindeki güven eksiklikleri olarak sayılabilmektedir. Veri koruma risklerinin en çok mobil aygıtlarda, ikincil olarak ise bulut bilişim alt yapısında ortaya çıktığı görülmektedir [10].

Bulut sistemlerde, farklı noktalarda bulunan bilgi, değişik bileşenler tarafından yönetilebilmekte, farklı coğrafi konumlarda bulunan sunucular üzerinde depolanmaktadır. Bu nedenle, veri ile ilgili uyumluluk gereksinimleri için küresel yasalara göre uzlaşmak zor olabilmektedir. Bu durumda; veriye sahip olma kısıtları, sektöre bağlı kısıtlar, ulusal veya eyalet bazındaki kısıtlar göz önüne alınmaktadır.

Bilişim teknolojileri açısından güvenilirlik, korunan veriye yalnızca yetkili kişilerin veya sistemlerin erişebilmesi ile sağlanmaktadır. Bulut üzerinde; bellek, ağ, veriler, uygulamalar çoklu kullanım ile paylaşılmaktadır. Bulut sistemlerinde, gün geçtikçe artan kullanıcı ve sistem sayısı ile birlikte sürekli yeni aygıtlar ve uygulamalar eklenmekte, erişim noktaları da artmaktadır. Bu nedenle; bulut sistemler üzerindeki güvenirlik, sisteme yeni bir erişim noktası eklendiği an tehdit altına girebilmektedir. Güvenilirliğin sağlanması için dikkat edilmesi gereken bir diğer unsur da korsan siteleridir. Bu amaçla, güvenlik servisleri kullanılmalıdır. Uçtan uca güvenlik, yalıtım ile sağlanabilmektedir. Bulutta yalıtım; bulut sağlayıcılarından tüm bileşenlerin, kullanıcıların ve kullanıcıların uygulamalarının yalıtılması anlamındadır. Bulut sağlayıcıları, kullanıcılarına güçlü ve kullanışlı bir yalıtım desteği sunmalıdır. Ancak, bulut mimariler üzerinde, yapıları gereği kullanıcılara sunulan servisler çoklu kullanıcılara da verilebilmektedir. Çoklu iş parçacığı yaklaşımı kullanılsa bile servisin yalnızca adres sahası paylaşılmalıdır. Böylelikle, bulut kullanıcılarına, verilerin güvende olduğu ve yetkisiz kullanıcıların işlem yapamayacağı bildirilmiş olmaktadır.

**3.1 Bulut Mimariler Üzerindeki Gizlilik**

# Riskleri

Bulut servisleri eğer kişisel bilgileri ele almaktaysa, bulut mimarisinde mahremiyet (privacy) kavramı da dikkate alınmalıdır. Kişinin bulunduğu yere, tercihlere, sosyal ağlara ve bu gibi dinamik bilgilere göre kişiselleştirilen bulut servisleri için yüksek bir mahremiyet tehdidi öngörülebilmektedir. Kişisel bilgilere ek olarak, kurumsal bilgilerin ve ticari sırların da ağ üzerinde paylaşımı dikkate alındığında gizlilik de önemsenmelidir [11]. Bulut mimarisi gereği, veriler çeşitli sunucularda depoladığından, bir ülkedeki kişilere ait verilerin bir başka ülkede barındırılması güvenlik tehdidi olarak oluşturmaktadır. Bu nedenle, ülkeler bulut kullanımıyla ilgili olarak kendi kanunlarını çıkarmaktadırlar [9].

**3.2 Bulut Mimariler Üzerindeki Veri Bütünlüğü Riskleri**

Veri bütünlüğü, veri üzerinde istenmeyen değişikliklerin önüne geçerek tutarsızlıkların oluşmasını engellemektir [9]. Geleneksel yöntemlerde veri bütünlüğünü sağlamak çok kolay olmaktadır. Çünkü, tek bir veritabanı üzerinde yapılan işlemlerin kontrolü kolaydır. Geleneksel veritabanları üzerinde ACID (Atomicity, Consistency, Isolation and Durability) ilkesi kullanılmaktadır. Bulut gibi dağıtık sistemlerde ise birçok veritabanı, birçok sistem ve birçok uygulama bulunmaktadır. Veri bütünlüğünün sağlanabilmesi için, veritabanları arası ya da sistemler arası erişimler ve veritabanları üzerinde yapılan işlemler dikkatli bir şekilde ele alınmalı ve yönetilmelidir. Bunu sağlamak için, merkezi veritabanı hareketi yöneticisi (central global transaction manager) kullanılmaktadır.

# 4. Bulut Sistemlerine Yönelik Saldırılar

Bulut Bilişim hizmet sağlayıcılarında meydana gelebilecek hizmet kesintileri, hizmet sağlayıcıları içindeki yazılımsal, donanımsal ya da mimari bir hatadan kaynaklanabileceği gibi, dışarıdan gelebilecek saldırılardan da kaynaklanabilmektedir. Bulut; birçok kullanıcı tarafından erişilebilir olduğundan, bu ataklara daha açıktır. Bu bölümde, bulut sistemlerine yönelik çeşitli saldırı tipleri açıklanmaktadır.

**4.1 Dağıtık Hizmet Engelleme Saldırıları (Distributed Denial of Service Attacks, DDoS)**

Dağıtık hizmet engelleme saldırıları, bilgi güvenliği unsurlarından erişilebilirliği (availability) hedef almaktadır. Sistemin kaldırabileceği yükün çok üzerinde anlık istek sonucunda anlık kullanıcı sayısı ile sistem yorulmakta ve cevap veremez hale getirilmektedir. DoS saldırıları, her zaman kapasite üstü istekle gerçekleştirilmeyebilir. Hedef sistemlerde bulunan zafiyetler de sistemin erişilebilirliği açısından risk oluşturabilmektedir. Saldırganlar, DDoS saldırıları düzenleyip, bulut bilişim hizmet sağlayıcıların hizmetlerini kesintiye uğratacakları tehdidi ile hizmet sağlayıcı firmalardan para talep edebilmektedirler [11]. Bu saldırılarda kullanılan bot adı verilen bilgisayarlar, bilgisayar korsanları tarafından zararlı yazılımlar yüklenip ele geçirilmiş ve kullanıcısının farkında olmadan istenildiği an istenen bir noktaya saldırması sağlanan bilgisayarlardır. Etkili hizmet dışı bırakma saldırılarının düzenlenebilmesi, hizmet sağlayıcılar için önemli bir tehlike ve risk oluşturmaktadır.

Ancak, bulut bilişim hizmet sağlayıcılarının bu tür saldırılara karşı koyacak koruma düzeneklerini oluşturma yoluna gitmesi, ihtiyaç anında hızlı ve dinamik kaynak ayırabiliyor olmaları sayesinde, gelen DDoS saldırılarına karşı koyabilmeleri, saldırının geldiği noktaları tespit edip engelleyebilmeleri mümkün olmaktadır [11].

**4.2** **Yan Kanal Saldırıları (Side**

# Channel Attacks )

Bulut bilişim mimarisindeki IAAS modeli, bulut altyapısını oluşturmaktadır. Bulut altyapısında; bilgisayar toplulukları, sanal makineler, uygulamalar, dosyalar, dokümanlar gibi genel kaynaklar bulunmaktadır. Örneğin, Amazon EC2 servisi kullanılarak, iç bulut yapısı tanımlanabilmekte ve sanal makinelerin konumlanması gereken yerler belirlendikten sonra internet aracılığı ile diğer topluluklarla ve sanal makinelerle iletişim kurulabilmektedir [12]. Bu saldırı tipinde, saldırgan bulut sunucusu içerisindeki kötü niyetli bir sanal makine içerisinde konumlanmakta ve iç bulutta belirlenen sanal makine aracılığı ile de gizli bilgilere erişebilmektedir. Bu saldırı tipi, diğer saldırılardan farklı olarak fiziksel bir gerçekleştirim sonucunda oluşmaktadır [12]. Saldırı iki aşamada gerçekleşmektedir. Birincisi yerleşme, ikincisi de verinin dışa aktarımıdır. Yerleşme, saldırganın saldıracağı sanal makinaya yerleşmesidir. Verinin dışa aktarımı ise, saldırgan aracılığı ile bilgilerin ele geçirilmesidir. Verilerin şifreli bir şekilde tutulmasının önemi bu saldırılarda ortaya çıkmaktadır. Saldırgan veriye erişmiş olsa bile, veri şifreli olduğunda çözememekte ve amacına ulaşamamaktadır [12].

**4.3 Ortadaki Adam Saldırıları (Man-In-The-Middle Attacks)**

Ortadaki adam saldırısında; saldırgan, kendisini iki kullanıcı arasında konumlandırmaktadır. Bu iki kullanıcı etkileşime geçtiği zaman diğer kullanıcıların erişimlerini koparabilmekte ve istediği bilgilere erişebilmektedir. Bu bağlantıyı koparmak ve yeni bağlantıyı sağlamak için kullanılan araç içinde yerleşik sertifika sistemi bulunmaktadır. Böylelikle, SSL bağlantıları taklit edilebilmekte, kişisel bilgiler saldırganın eline geçebilmektedir.

# 5. Bulut Saldırılarından Korunmak için Geliştirilen Yöntemler

Bulut bilişim, çoklu kullanıcı desteği ve sanallaştırma özelliklerinden dolayı ölçeklenebilirliği sağlamaktadır. Bulut, bir yazılımı bir kişiyle paylaşmak yerine, bir yazılımı birçok kullanıcı tarafından erişilebilir kılmaktadır. Bu durumda, özellikle dikkat edilmesi gereken bazı noktalar ortaya çıkmaktadır. Belirtilen kontrolleri bulutta sağlamak için, geleneksel yöntemler işe yaramamaktadır. Çünkü; sunucular, aynı güvenilir alt birim içindeki erişim kontrol düzeneklerinden sorumludurlar ve geleneksel yöntemler uygulama merkezli erişim kontrolüne sahiptirler. Böylelikle, her uygulama kendisine erişebilecek kullanıcıları ve bu kullanıcıların yeteneklerini bilmektedir.

Bir uygulama diğer uygulamalar tarafından paylaşılabilmekte ve veri kopyalama gerçekleşebilmektedir. Bu kontrollerin bulutta yapılması oldukça güçtür.

**5.1 Kimlik Yönetimi ve Kullanıcı**

# Doğrulama

Bulut üzerindeki her bilgi, kişilerin ya da kurumların bulut üzerinde kiraladıkları yerlerde saklanmaktadır. Kullanıcı, bilgilerine nereden ve nasıl erişmek isterse, kullanıcı girişi sırasında kullanıcı doğrulanmakta ve onaylanmaktadır [13]. Bulut sistemleri sayesinde, kullanıcılar kendi kişisel bilgilerine internet olan herhangi bir ortamdan erişebilmektedir ve bu erişim, kimlik yönetim sistemi ile sağlanmaktadır. Bu mekanizma, kullanıcıların servis tabanlı hizmetler aracılığı ile kullanıcı adı ve şifrelerini doğrulayarak, kullanıcıya kendi kişisel bilgilerine erişme izni vermektedir [4]. Kullanıcı doğrulama servisleri, üçüncü parti sistemler ile bütünleştirilmek istendiğinde gizlilik protokolleri kullanılmaktadır. Bu protokollere örnek olarak verilen *Sıfır Bilgi İspatı* *(ZeroKnowledge Password Proof)*, genellikle şifreleme algoritmalarında kullanılan ve şifrenin korunduğu ve doğrulamanın bu şekilde yapılabildiği bir tekniktir. Bulut sistemler üzerinde bu tekniğin kullanılması, bazı kullanıcı saldırılarını önlemektedir [4]. Birçok şirket kendi çalışanlarının bilgilerini LDAP

(Lightweight Directory Access Protocol) sunucularında tutmaktadır. Erişimlerin yönetimi ise AD (Active Directory) sunucularında bulunmaktadır. Şirketler, bulut üzerinde kiraladıkları sunucularda çalışan erişim bilgilerini bulundurmak istememektedir. Bu durumda, LDAP/AD sunucuları, bulut hizmeti dışında bırakılabilmekte ve erişim gerektiği zamanlarda bu sunucularla iletişime geçerek çözüm sağlanmaktadır [2]. Doğrulama saldırılarının önüne geçmek için bazı firmalar sanal klavyeler, gizli sorular ya da anahtarlar gibi ikinci bir önlem almaktadır.

## 5.2 Erişim Kontrolü

Bilgi güvenliğinin sağlanması ve için en önemli maddelerden biri erişim kontrolleridir. Erişim kontrolünü etkin ve efektif olarak uygulamak başta veri kaybı olmak üzere birçok konuda daha güvenli bir yapıda olmayı sağlamaktadır. Erişim kontrollerinin bulut sistemler üzerine uygulanması ile daha güvenilir bir sistem elde edilmektedir. Sistem güvenliğinin kaynakların ve verinin korunmasının ilk yolu, sistemin kendine gelen erişimleri kontrol altında tutmasıdır. Erişim kontrolü, sadece kullanıcıların herhangi bir kaynağa erişimini yönetmesi değildir, aynı zamanda; kullanıcıları, dosyaları ve diğer kaynakları da yönetmelidir. Yetkisiz erişimlerin denetlenmesi ile birlikte veri ve sistem bütünlüğünün korunması amaçlanmaktadır. Erişimlerin yetkilendirilmesi ve işlemlerin günlük (log) kayıtlarının tutulması ile, veri üzerinde kimlerin değişiklik yaptığı görülebilmektedir. Böylelikle, sistemin görülebilirliği artmaktadır [9].

Veri paylaşımı, verinin güvenliğini sağlamada dikkat edilmesi gereken bir diğer maddedir. Veri sahibi, bir gruba veri paylaşım izni verdiğinde, izin verilen grubun bu veriyi başka hangi gruplara iletebileceği göz önünde bulundurulmalıdır. Paylaşım politikaları ile hassas bilginin orijinal veriden yalıtılması sağlanabilmektedir. Paylaşım politikaları kullanılarak, verinin sahibinden bağımsız bir şekilde yönetilebilmesi sağlanmaktadır [5]. Bulut sistemlerinde yaygınlıkla kullanılan erişim kontrol mekanizması Rol Temelli Erişim Kontrolü [14] (Role-based

Access Control, RBAC)’dür. Bu mekanizmanın kullanılmasının nedenleri arasında; RBAC’in kullanım kolaylığı, dinamik gereksinimlere ayak uydurabilme özelliği, en az yetki prensibine dayanması ve ayrıcalıkların dinamik kontrolü belirtilmektedir.

## 5.3 Veri Şifreleme

Veri güvenliğini sağlamanın en genel çözümü veri şifreleme olarak bilinmektedir. Şifrelemenin etkinliğinden emin olmak için şifreleme algoritmaları ile birlikte şifreyi açacak anahtarın da dayanıklılığı önem kazanmaktadır. Bulut ortamlarında çok büyük veri aktarımları, veri üzerinde işlemler, veri depolama ve yönetme işlemleri olduğundan, işlem hızı da şifreleme algoritmaları tasarlanırken önem kazanmaktadır. Bulut sistemlerde bu nedenle asimetrik şifreleme algoritmaları yerine, simetrik şifreleme algoritmaları kullanılması daha uygun bulunmaktadır [5]. Veri güvenliği şifreleme algoritmaları ile güçlendirilse de, bu algoritmaları çözecek anahtarın yönetimi zayıf olduğunda veri güvenliği sağlanamamaktadır. Bu nedenle, anahtar verisinin sahibi anahtarı korumakla yükümlü olmaktadır. Anahtar verisinin korunması da veri güvenliği kapsamında değerlendirilmektedir. Ancak, anahtarlar bulut sağlayıcılarına emanet edilmektedir. Bulut üzerinde anahtar yönetimi, kullanıcı sayısının çok olması ve sistemin karmaşık olmasından dolayı karmaşık ve zordur [5].

Mobil bulut sistemlerinde hesabın çalınmasına önlem olarak, dinamik şifre belirleme algoritmaları kullanılmaktadır.

Bu algoritmada; kullanıcı, yer değiştirdiğinde ya da belirli sayıda veri paketi alışverişi yaptığında, dinamik olarak şifre de değişmektedir [6].

Bulut üzerindeki uygulamalar internet üzerinden bir web tarayıcı aracılığıyla indirilmektedir. Saldırgan kullanıcının bilgisayarına yerleşip, bilgi hırsızlığı yapabilmektedir. Bunu engellemek için RSA gibi şifreleme algoritmalarıyla birlikte dijital imza da kullanılmaktadır.

Ek olarak; Açık Web Uygulaması

Güvenlik Projesi (Open Web Application Security Project, OWASP) geliştirilmiş olup, en önemli on güvenlik tehdidi belirlenmiştir [6]. Bulut Güvenlik Birliği (The Cloud Security Alliance, CSA) bu konuda bir doküman hazırlamış ve sıklıkla karşılaşılan tehditleri belirlemiştir. Bu doküman içinde; merkezi bir sözlük, erişim yönetimi, kimlik yönetimi, rol tabanlı erişim kontrolü, kullanıcı erişim sertifikaları, ayrıcalıklı kullanıcı ve erişim yönetimi gibi bilgiler bulunmaktadır.

 **5.4 Veri Aktarımı**

Veri güvenliği ve bütünlüğünü sağlama yöntemlerinden bir tanesi veri aktarımlarının belirli aktarım protokolleri üzerinden yapılmasıdır. Böylelikle veri aktarımı sırasında herhangi bir kayıp yaşanması önlenmektedir [5]. Verinin arşivlenmesi, taşınabilir saklama aygıtları yerine sabit saklama aygıtlarında tutulmakta ve bu şekilde verinin kaybolma riski azalmaktadır. Ancak, fiziksel aygıtların doğası gereği, belli bir süre sonra bozulabilmekte ve içerdiği tüm bilgiler silinebilmektedir. Belirtilen bu durumlar dışında, güvenliğin artırılması için aşağıda açıklanan adımlar izlenmelidir:

* İşletim sisteminin, programların ve tüm veri dosyalarının belli aralıklarla yalıtılması ile erişilebilirlik ilkesi güçlendirilmelidir.
* Yedekleme ağının ana trafikten veya ana çalışma alanından ayrılması ile ilgili trafikteki izinsiz kullanıcıların yedek dosyalara erişimi engellenmelidir.
* Yedekler de güvenli bir yerde tutulmalıdır.
* Bulut akıllı ağları kurularak ve IAAS kullanılarak, bulutun güvenli bir şekilde uzak sitelere de bağlanabilmesi sağlanmalıdır.
* Buluta yapılan bağlantının güvenli olması için politikalar kullanılmalıdır.
* Bulut bilişim sağlayıcısı, müşterilerine; veri işlemesi, verinin kullanılması, verinin yeri gibi konuları açıkça belirtmeli ve bu maddeler kontrata eklenmelidir [13].
* Yeterli günlük kayıtları ve denetleme sağlanarak müşterinin güveni artırılmalıdır [13].
* Son kullanıcı gibi profesyonel olmayan kullanıcılara yönelik eğitimler hazırlanmalı ve bulut hizmetinden yararlandıkları sürede hangi bilgilerinin hangi koşullar altında buluta aktarılacağı konusunda bilgilendirilmelidirler [13].
* Bulut üzerine çalışan kişiler, yeni risk tiplerini analiz etme ve yönetebilme yeteneğine sahip olmalıdır [13].

# 6. Sonuç

Bulut bilişim bilgisayar dünyasına önemli bir katkıda bulunmaktadır. Özellikle mobil bulut teknolojileri sayesinde, bulut teknolojileri ve mobil teknolojilerinin avantajlarının harmanlanması sağlanmış ve eğilim haline gelmiştir. Mevcut sistemleri bulut içine geçirmek kolay bir iş olmamakla birlikte, dikkatli planlama ve yükleme ile maliyetleri önemli ölçüde düşüren bir yöntem olarak kullanılmaktadır. Bulut sistemler, yapısı gereği, paylaşılan kaynak kullanmaktadır. Paylaşılan kaynaklar; ağ, sunucular, depolama birimleri, uygulamalar veya servisler olabilmektedir. Bu paylaşımlı altyapı sunumu, birçok güvenlik tehdidini de beraberinde getirmektedir. Bu güvenlik tehditlerini en aza indirmek için yöntemler geliştirilmeli ve bulut sistemler ile bir arada kullanılmalı, yazılımlar birbirinden soyutlanmalı ve sürekli geliştirilebilir olmalıdır.

# 7. Kaynaklar

1. L.A. Martucci et al., “Privacy, security and trust in cloud computing: the perspective of the telecommunication industry”, **The 9th Int. Conf. on Ubiquitous Intelligence Computing and Autonomic Trusted Computing (UIC/ATC)**, 627–632 (2012).

1. S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, **Journal of Network and Computer Applications**, 34(1), 1-11 (2011).
2. N. Kshetri,"Privacy and security issues in cloud computing: The role of institutions and institutional evolution", **Journal Telecommunications Policy**, 37(4-5), 372-386 (2013).

1. H. Takabi , J. B. D. Joshi , G.-J. Ahn, “Security and Privacy Challenges in Cloud Computing Environments”, **IEEE**

**Security and Privacy**, 8(6), 24-31 (2010).

1. İ. Korkmaz, F. Tekbacak, “Bulut Hesaplama Güvenliği, Genel Bir Bakış”, **Akademik Bilişim Konferansı** (2013).

1. K. Hashizume et al., “An analysis of security issues for cloud computing”, **Journal of Internet Services and Applications**, 4(5), 1-13 (2013).

1. A. Korn et al., "A Service Level Management Authority in the Cloud", **HP Laboratories Technical Report**, http:// www.hpl.hp.com/techreports/2009/HPL2009-79.pdf (Son Erişim Aralık 2014).

1. Microsoft SQL Azure Service Level Agreement, http://azure.microsoft.com/enus/support/legal/sla/ (Son Erişim Aralık 2014).

1. D. Zissis, D. Lekkas, "Addressing cloud computing security issues", **Journal Future Generation Computer Systems**, 28(3), 583-592 (2012).

1. A. C. Donald, S. A. Oli, L. Arockiam, “Mobile Cloud Security Issues and Challenges: A Perspective”, **Int. J. of Engineering and Innovative Technology (IJEIT)**,3(1),401-406 (2013).

1. S. Pearson, S., "Privacy, Security and Trust in Cloud Computing", **Privacy and Security for Cloud Computing Computer Communications and** **Networks**, 3-42 (2013).

1. B., “Security against Side Channel Attack in Cloud Computing”, **Int. J. of Engineering and Advanced Technology (IJEAT)**, 2(2) (2012).

1. M. Hölbl, “Cloud Computing Security and Privacy Issues”, **The Council of European Professional Informatics Societies (CEPIS)**, http://www.cepis.org/ media/CEPIS\_Cloud\_Computing\_Security \_v17.11.pdf (Son Erişim Aralık 2014).

1. D. F. Ferraiolo, D. R. Kuhn, R. Chandramouli, “Role Based Access Control”, **Artech House Publishers**, 2nd Edition, ISBN 13: 978-1-59693-113-8 (2007).