BULUT BİLİŞİMDE GÜVENLİK ZAFİYETLERİ, TEHDİTLER VE BU TEHDİTLERE YÖNELİK GÜVENLİK ÖNERİLERİNİN İNCELENMESİ

Işıl KARABEY AKSAKALLI
Erzurum Teknik Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Erzurum, 25050, Türkiye

ÖZET

Bulut bilişim, yeni çağı simgeleyen paralel hesaplama, dağıtık hesaplama ve sanallaştırma teknolojilerinin gelişimidir. Bu teknoloji, talep üzerine internet altyapısına inşa edilip bulut üzerinden yazılım, uygulama, iş ve tüketici bilgi teknolojileri (BT) hizmetleri sunan esnek, uygun maliyetli ve yapılandırılabilir hesaplama kaynaklarına sahip popüler bir teknolojidir. Bulut bilişimin esnek altyapısı, ağ merkezli yaklaşımı ve erişim kolaylığı sebebiyle küçük, orta ve büyük ölçekli birçok organizasyon tarafından kullanımı giderek yaygınlaşmaktadır. Fakat çoklu kiracılık, kaynak paylaşımı ve dış kaynak kullanımı, veri ve hizmet alımını üçüncü bir taraftan sağlama gibi bulut bilişimin getirdiği yeni kavramlar, bazı güvenlik risklerini de beraberinde getirmektedir. Bu zorlukların üstesinden gelmek, geleneksel bilgisayar sistemleri için geliştirilen güvenlik önlemlerini geliştirme ve ayarlama yeteneği ile birlikte bulut güvenliği zorluklarını ele almak için yeni güvenlik politikaları, modelleri ve protokolleri önermeyi gerektirmektedir. Bu çalışmada bulut bilişimde meydana gelen güvenlik zafiyetleri ve bu zafiyetler kullanılarak bulut sistemlerine yapılan saldırı türleri üzerine kapsamlı bir çalışma sunulmuştur. Literatürde yer alan bulut güvenlik zafiyetleri tespit edilerek bulut bilişimin maruz kaldığı güvenlik tehditleri ve saldırılar sınıflandırılmıştır. Ayrıca güvenlik açıklarını kontrol etmek, sınıflandırılan bu tehditlerin etkisini en aza indirgemek ve saldırıları kalibre etmek için alınan güvenlik önlemleri literatür çalışmaları ile desteklenerek açıklanmıştır.

Anahtar Kelimeler— Bulut bilişim, Bulut güvenliği, Bulut zafiyetleri, Güvenlik tehditleri, Bulut güvenliği için çözüm önerileri

Security Vulnerabilities, Threats in Cloud Computing and The Examination of Security Measures Against These Threats

ABSTRACT

Cloud computing is a development of parallel and distributed computing and also virtualization technologies symbolizing the new era. It is a popular technology with flexible, cost-effective and configurable computing resources that construct to internet on-demand and present software, application, business and consumer information technology services through cloud. Because of flexible infrastructure, network centric approach and accessible cloud's usage is becoming increasingly widespread. But the new concepts brought by cloud computing, such as providing multiple tenancies, resource sharing and outsourcing, data and service procurement from a third party, bring with it some security risks. Overcoming these challenges requires the introduction of new security policies, models and protocols to address cloud security challenges, along with the ability to develop and adjust security measures for traditional computer systems. In this study, a comprehensive study on the security vulnerabilities in cloud computing and the types of attack on cloud systems are presented. Cloud security vulnerabilities found in the literature have been identified and security threats and attacks against cloud computing have been classified. In addition, security measures to control the security vulnerabilities, to minimize the impact of these threats and to calibrate the attacks are described supporting with the literature.

Keywords— Cloud computing, Cloud security, Cloud vulnerabilities, Security threats, Trends solution for cloud security

I. GİRİŞ (INTRODUCTION)

Bulut bilişim, uygulamaların internet ortamında barınmasını ve "kullandıkça öde" stratejisi ile kullanıcıların yalnızca tükettiği hizmet birimi kadar ödeme yapmalarını sağlayan sanallaştırılmış ve ölçeklenebilir kaynakların toplamıdır [1]. Bu teknoloji, kullanıcıların veri ve uygulamalarını uzak "Bulut" sistemine taşıyarak istedikleri zaman basit ve hızlı bir şekilde kaynaklara erişimini sağlayan bir sistemdir. Bulut bilişim modelinin en yaygın kullanılan tanımı NIST [3] tarafından "Minimum yönetim çabası veya servis sağlayıcı etkileşimi ile hızla tedarik edilebilen ve serbest bırakılabilen, paylaşılabilir ve yapılandırılabilir hesaplama kaynakları havuzuna uygun (örneğin ağlar, sunucular, depolama, uygulamalar ve servisler), isteğe bağlı ağ erişimini sağlamak için bir model" şeklinde yapılmıştır.

2007 yılının sonlarına doğru üretilen Bulut Bilişim teknolojisi kullanılarak, bugüne kadar endüstri ve akademik alanda RESERVOIR (IBM ve Avrupa Birliği'nin Bulut bilişim için ortak araştırma girişimi), Amazon Elastic Compute Cloud ve IBM şirketinin Blue Cloud projesi başlatılmıştır [72]. Ayrıca Nimbus, Stratus, OpeNEbula, HP, Intel Corporation and Yahoo! gibi birçok bilimsel proje; endüstri, araştırma ve eğitim için açık kaynak bulut bilişim test ortamı, küresel ve çoklu veri merkezinin oluşumu olarak duyurulmuştur [72].

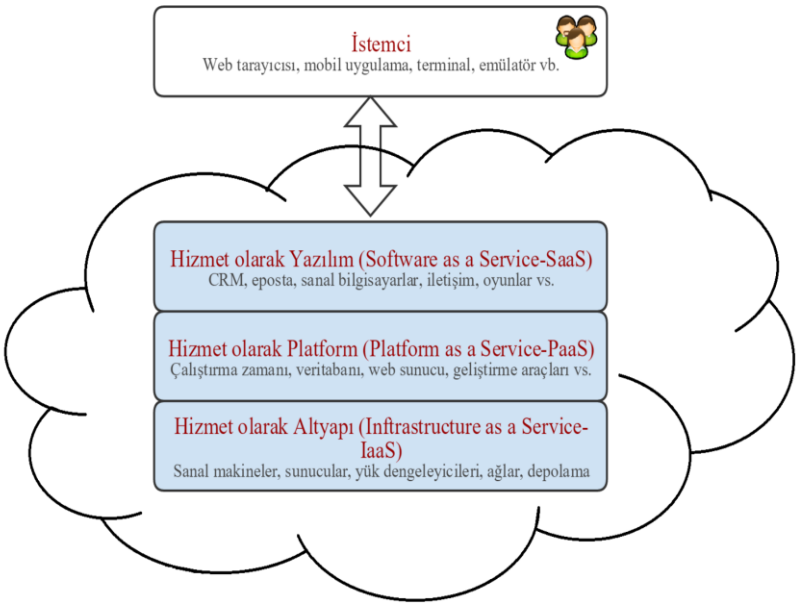
Bulut bilişim, kullanıcıların yazılım ve verilerinin sunucular üzerinde depolanmasını sağlarken aynı zamanda bilişim ihtiyaçlarını karşılamak için internet (web) tarayıcıları aracılığıyla çevrimiçi yaygın iş uygulamaları sağlamaktadır. Böylece Hizmet Odaklı Mimari (Service Oriented Architecture), Web 2.0, sanallaştırma ve internete bağlı diğer teknolojiler bir takım hesaplama kavramlarını ve teknolojileri birleştirmektedir [6]. Bulut bilişimden elde edilen potansiyel kazanımlara rağmen, bu teknoloji nispeten yeni bir hesaplama modelini temsil ettiği için her seviyede güvenliğin nasıl elde edilebileceği ve uygulama güvenliğinin bulut ortamında nasıl sağlandığı konusunda bir belirsizlik bulunmaktadır [6]. Bu belirsizlikten dolayı model güvenliğine duyulan şüphe, bulutun benimsenmesini etkilemekte ve bulut bilişim pazarının ilerlemesine engel olmaktadır [1, 11].

Bu çalışmada, bulut bilişimin katmanlı mimarisi değerlendirilerek bu katmanlı mimaride meydana gelen güvenlik problemleri ve bu problemlere yönelik literatürde önerilen çözümler üzerine bir derleme çalışması yapılmıştır. Makalenin geri kalan kısımları şu şekilde düzenlenmiştir: 2. Bölümde bulut bilişim mimarisi hakkında bilgi verilmiştir. 3. Bölümde bulut platformunun katmanlı yapısından kaynaklanan güvenlik zafiyetleri, bu zafiyetler kullanılarak yapılan saldırılar ve bunlar arasındaki ilişki detaylı bir şekilde incelenmiş ve sınıflandırılmıştır. 4. Bölümde ise geniş kapsamlı bir literatür araştırması yapılarak bulut bilişimde gerçekleşen saldırılara karşı önerilen güvenlik yöntemlerine yer verilmiştir. 5. Bölümde ise sonuç ve öneriler üzerinde durulmuştur.

II. BULUT BİLİŞİM MİMARİSİ (CLOUD COMPUTING ARCHITECTURE)

Kavramsal olarak kullanıcılar, Bulut bilişimden BT (Bilgi Teknolojileri) altyapıları ya da hesaplama platformları edinmekte ve onları kendi uygulamaları içerisinde çalıştırmaktadır. Kullanıcıların yalnızca ihtiyaç duydukları hizmetleri kullanmaları için bulut bilişimin alt yapısı Şekil 1'de görüldüğü gibi (a) Hizmet olarak yazılım (Software as a service-SaaS), (b) Hizmet olarak platform (Platform as a service-PaaS) ve (c) Hizmet olarak altyapı (Infrastructure as a service-IaaS) olmak üzere üç katmana ayrılmaktadır. Bu katmanlı yapı, kullanıcılara donanım, yazılım ve veri kaynakları sağlamakta, daha sonra da entegre edilmiş hizmet olarak hesaplama platformuna şeffaf bir şekilde erişmek için çeşitli hizmetler sunmaktadır.

IaaS (Infrastructure-as-a-service) modeli, bulut fiziksel altyapı katmanını (depolama, ağlar ve sunucular), sanallaştırma katmanını (hypervisor) ve sanallaştırılmış kaynaklar katmanını (sanal makineler (VMs), sanal depolama alanı, sanal ağlar) kapsamaktadır [5]. Tüketiciye işleme, depolama, ağ ve diğer hesaplama kaynaklarını sunarak kullanıcının işletim sistemleri ve uygulamaları içerebilecek rastgele yazılımlar çalıştırmasına ve dağıtmasına olanak tanımaktadır. Bu altyapıyı kullanan tüketici; işletim sistemleri, depolama, dağıtık uygulamalar ve belirli ağ bileşenlerinin sınırlı denetimi üzerinde kontrol sahibi olmaktadır [73].



Şekil 1. Bulut hizmeti dağıtım mimarisi

PaaS (Platform-as-a-service) modeli, platform katmanlarını (uygulama sunucuları, web sunucuları, IDE'ler ve diğer araçlar gibi) ve API'leri kapsamaktadır [5]. Hizmet sağlayıcı tarafından desteklenen programlama dilleri ve araçları ile, tüketici tarafından oluşturulan veya edinilen uygulamaların bulut altyapısı üzerinde dağıtılmasını sağlamaktadır. Tüketici bu katmanda IaaS katmanında yer alan ağ, sunucular, işletim sistemleri ya da depolamayı içeren bulut altyapısı ile ilgilenmemekte, dağıtım yapılan uygulamaları ve uygulama barındırma ortamı yapılandırmalarını kontrol edebilmektedir [73].

SaaS (Software-as-a-service) modeli, Şekil 1'de gösterildiği gibi SaaS, son kullanıcılar için bir hizmet olarak sunulan uygulamaları ve hizmetleri kapsamaktadır. SaaS katmanı, hizmetleri barındıracak bir platform katmanına ve çoklu kullanıcılara hizmet sunarken kaynak kullanımını optimize etmek için bir sanallaştırma katmanına bağlıdır [5]. Bir bulut altyapısı üzerinde çalışan sağlayıcı uygulamalarının tüketici tarafından kullanımını sağlamaktadır. Bu hizmet modelinde uygulamalar, web tabanlı elektronik posta gibi bir arayüz aracılığı ile birçok istemci cihazdan erişilebilir haldedir. Tüketici platform katmanında olduğu gibi sınırlı kullanıcıya özel uygulama yapılandırma ayarları hariç olmak üzere bireysel uygulamalar da dahil, ağ kaynakları, depolama, sunucu, işletim sistemlerinin olduğu bulut altyapısını yönetme ve kontrol etme işleri ile ilgilenmemektedir [73].

Bulutlar ayrıca istemci, uygulama, platform, altyapı ve sunucuları içeren beş bileşenli mimariler olarak görülmektedir [8]. Mevcut bulutlar [11, 14];

- Hizmet sağlayıcısı tarafından yönetildiği ve sürdürüldüğü fiziki altyapıya sahip açık bulutlar (public clouds): Genel kullanıcıların mevcut altyapıya kayıt olma ve altyapıyı kullanmaları için geliştirilen bir bulut platformu
- Fiziki altyapının bir organizasyonlar birliği tarafından yönetildiği ve sürdürüldüğü topluluk bulutları (community clouds),
- Altyapının belirli bir kuruluş tarafından yönetildiği ve sürdürüldüğü özel bulutlar (private clouds) ve
- Yukarıdaki üç modelin kombinasyonlarını içeren hibrit bulutlar (hybrid clouds): Genel bulutlarda kaynakları kullanacak şekilde genişletilebilen özel bir bulut platformu

olmak üzere dört farklı dağıtım modelinden birinde dağıtılmaktadır.

Bulut modelinin kullanılması durumunda hesaplamaların dışarıya aktarılması, kaynak paylaşımı ve dış veri ambarı gibi bulutlar tarafından sunulan yeni kavramlar, güvenlik ve gizlilik kaygılarını artırmakta ve yeni güvenlik zorlukları yaratmaktadır. Ayrıca bulutların

büyük bir kısmının mobil erişim aygıtlarına taşınması ve bulut altyapısına doğrudan erişimin sağlanabilmesinden dolayı bulut güvenlik zafiyetleri ve tehditleri giderek artmaktadır [8].

III. BULUT BİLİŞİMDE GÜVENLİK PROBLEMLERİ (SECURITY PROBLEMS IN CLOUD COMPUTING)

Bulut Güvenlik Birliği (Cloud Security Alliance-CSA) tarafından 2010 yılında yayınlanan raporda bulut kullanıcıları, güvenlik risklerinden haberdar edilmiştir. Bu raporda bulut bilişimi tehlike altına alan yedi ana tehditten bahsedilmektedir. CSA, önem derecesine göre yayınlandığı bu tehditlerin önlenebilmesi için bazı iyileştirme önerilerinde de bulunmuştur. Bahsedilen yedi güvenlik tehdidi önem derecesine göre aşağıdaki gibi sıralanmıştır [2]:

- Bulut bilişimin suistimal edilmesi ve kötüye kullanımı
- Güvenilir olmayan uygulama programlama ara yüzleri
- İçerideki kötü niyetli kişiler
- Paylaşılan teknoloji zayıflıkları
- Veri sızıntısı/kaybı
- Hesap, hizmet & trafik kaçırma
- Bilinmeyen Risk Profili

2010 yılından itibaren bulut kullanımının artması ile CSA, 2013 yılında raporu düzenlenmiştir ve özellikle veri kaybı ve veri ihlali farklı kategorilere ayrılarak en önemli iki problem haline gelmiştir [3].

a) SPI (Software-Platform-Infrastructure) Modelinde Güvenlik (Security on SPI model)

Bulut bilişimde güvenlik zorlukları analiz edilmeden önce üç katmanlı bulut hizmet modelleri arasındaki bağlılığı ve ilişkiyi anlamak gerekmektedir [4]. PaaS ve SaaS, IaaS'nin üzerinde bulunduğu için IaaS'deki herhangi bir ihlal, hem PaaS hem de SaaS hizmetlerinin güvenliğini etkilemektedir. Aynı zamanda birbirlerine bağlı modeller oldukları için bu durumun tersi de söz konusudur. Modeller arasındaki derin bağlılıktan dolayı herhangi bir bulut katmanına yapılan bir saldırı üst katmanları da olumsuz etkilemektedir [6].

Çalışmanın 2. bölümünde bahsedilen katmanlı yapıdan en üst seviyede bulunan SaaS ile güvenliğin yükü bulut sağlayıcıya uzanmaktadır. Kısmen bu durum, soyutlama derecesinden kaynaklanmaktadır ve SaaS modeli minimum müşteri kontrolü ya da genişletilebilirlik ile entegre edilmiş işlevsellik üzerine kuruludur. Aksine PaaS modeli ise daha fazla genişletilebilirlik ve daha fazla müşteri kontrolü sunmaktadır. Büyük ölçüde soyutlama derecesi daha düşük olduğundan IaaS, güvenlik üzerinden PaaS ya da SaaS'a göre daha fazla kiracı ve müşteri kontrolü sunmaktadır [6].

b) Hizmet olarak Yazılım (SaaS) Güvenlik Problemleri (Security problems in Software as a Service-SaaS)

SaaS talep üzerine elektronik posta, konferans ve ERP, CRM ve SCM gibi iş uygulamalarını kullanıcılara sağlamaktadır. SaaS kullanıcıları bulutta bulunan üç temel teslim modeli arasında en az güvenlik kontrolüne sahip katmandır [6]. SaaS uygulamalarına adaptasyon aşağıda verilen bazı güvenlik kaygılarını da beraberinde getirmektedir:

Uygulama Güvenliği:

İnternet üzerinden son kullanıcılara BT uygulamaları teslim eden bir hizmet modeli olan SaaS modelinde web uygulamalarındaki kusurlar bazı zafiyetlere sebebiyet vermektedir [38]. Saldırganlar interneti kullanarak kullanıcıların bilgisayarlarını tehlikeye atmak ve hassas verileri çalmak gibi kötü amaçlı faaliyetler gerçekleştirmektedir. Örneğin, saldırganlar tarafından web uygulamalarında kullanılan SOAP (Simple Object Access Protocol-Basit Nesne Erişim Protokolü) gibi web servislerin mesaj başlığı, geçersiz istekler içermesi için manipüle edilebilmektedir [7]. Bu katmandaki güvenlik problemleri klasik bir web uygulamasından farklı olmasa da geleneksel güvenlik çözümleri SaaS modelini saldırılardan etkili bir şekilde koruyamamaktadır. Bu yüzden yeni yaklaşımlara olan ihtiyaç gün geçtikçe artmaktadır.

Çoklu Kiracılık (Multi-Tenancy):

SaaS uygulamaları ölçeklenebilirlik, üst veri (meta-data) yoluyla yapılandırılabilirlik ve çoklu kiracılık özelliklerine göre belirlenen olgunluk modellerine göre gruplandırılabilmektedir [6]. İlk olgunluk modelinde her müşterinin kendine özgü özelleştirilmiş yazılımı vardır. Bu modelin kaynakları etkin kullanamama, ölçeklenebilir olmama vb. dezavantajları vardır, fakat diğer modeller ile karşılaştırıldığında güvenlik açısından daha iyi bir durumdadır. İkinci

modelde satıcı her bir müşteri için farklı uygulama örnekleri sağlamakta, fakat tüm örnekler aynı uygulama kodunu kullanmaktadır. Bu modelde müşteriler ihtiyaçlarını karşılamak için bazı yapılandırma ayarlarını değiştirebilmektedirler. Üçüncü olgunluk modelinde ise çoklu kiracılık özelliği eklendiği için tek bir örnek tüm müşterilere hizmet etmektedir. Bu yaklaşım kaynakların daha verimli kullanılmasını sağlamakla birlikte ölçeklenebilirlik kısıtını da beraberinde getirmektedir [6]. Herhangi bir paylaşılan hizmette olduğu gibi, çoklu kiracılık modelinde de kiracılar birbirlerinden tamamen izole edilememektedir. Çoğu bulut hizmeti sağlayıcısı, farklı düzeylerde hizmet sunmak, sanal makineleri paylaşmak veya bir sanal makinenin tek bir kullanıcıya tahsis edildiği istemcileri ayırmak için sanallaştırma kullanmaktadır [39]. Yine de, bir kullanıcının çalışma şekli, aynı hizmetteki diğer kullanıcıları etkileyebilmektedir. Örneğin, kaynakları aşırı kullanmak veya kilitlemek, hizmetin kullanılabilirliğini etkileyen ve DoS (Denial of Service-Hizmet Aksatma) saldırılarına neden olabilen yaygın bir problemdir [4]. Bir başka problem ise çoklu kiracılıktan kaynaklanan depolama maliyetini düşürmek için bulut hizmet sağlayıcılarının (Dropbox, Oracle, IBM, Microsoft, EMC vb.) veri tekilleştirme (deduplication) yapmalarıdır [40]. Veri tekilleştirmede aynı verinin sadece bir kopyası bulutta saklanmaktadır [41]. Bu yöntem "istemci-taraflı veri tekilleştirme" adı altında istemci tarafında da uygulanmaktadır. Müşteriler verinin şifresini (hash) göndererek verinin varlığını kontrol etmekte ve bu işlem sonucunda veri bulutta yok ise depolanmaktadır. Böylece bant genişliği ve depolama tüketimi azalmaktadır. Bu yöntem bulut sağlayıcılar ve kullanıcılar için her ne kadar avantajlı görünse de saldırganlar, tahmin edilebilir mesajların şifresini tahmin ederek belirli bir bulutta depolanan dosyanın varlığını öğrenebilmektedir [40]. Ayrıca, kullanıcıların buluttan yararlandıkları ortam, sunucuyu ve diğer kullanıcıları etkileyebilir. Kötü amaçlı yazılım, sunucu vasıtasıyla yayılabilir, uygulamalara bulaşabilir ve diğer kullanıcılara geçebilir. Sanal ortamlar, sanal makineler arasında bir makineden daha fazla koruma sağlar, ancak yine de tamamen izolasyon sağlamazlar [4].

Veri Güvenliği:

Veri güvenliği herhangi bir teknoloji için ortak bir problem haline gelmekle birlikte SaaS kullanıcıları uygun güvenlik için bulut sağlayıcılarına güvenmek zorundadır. Verinin işlenip depolanmasından sorumlu kişilerden biri SaaS sağlayıcıdır [12]. Verinin bulutta depolanması, veri sızıntısını ve yetkisiz erişim riskini artırmakta, bu da sorumlu SaaS sağlayıcısına güveni azaltmaktadır. Ayrıca bulutta veri depolama, yedekleme, veri göçü, silme, güncelleme, arama, sorgulama ve erişim gibi işlemler bazı güvenlik endişelerini de beraberinde getirmektedir [6] [42]. Bunun nedeni ise bulut sağlayıcıların bu işlemleri sözleşme yaptığı üçüncü taraf servis sağlayıcıları ile işbirliği içerisinde yapmasıdır. İşlemlerin, tamamen güvenmenin mümkün olmadığı bir başka sağlayıcıya aktarılması, güvenlik endişelerini artırmaktadır [42].

Erişilebilirlik:

Mobil cihazlar aracılığı ile web tarayıcılar (browser) kullanılarak internet üzerinden uygulamalara erişmek, herhangi bir ağ cihazından daha kolaydır. Bununla birlikte bu kolaylık, kullanıcıları ek güvenlik risklerine maruz bırakmaktadır. CSA'nın yayınladığı raporda mobil bulut bilişimin mevcut durumu ve mobil zararlı yazılım ile bilgi çalma, güvensiz ağlar (WiFi), işletim sisteminde bulunan zafiyetler ve resmi uygulamalar, güvensiz pazarlar ve yakınlık tabanlı saldırılar gibi bu alandaki en büyük tehditler açıklanmıştır [14]. Bulut sistemine sahip Amazon, lisans sözleşmesinde açıkça, hizmete zaman zaman erişilemeyeceğini belirtmiştir [13].

Bir açık bulut altyapısındaki SaaS modelindeki güvenlik kaygılarına sebep olan en yaygın saldırıların başında erişilebilirlik gelmektedir. Erişilebilirlik ve diğer güvenlik tehditlerinin sebebiyet verdiği saldırılar aşağıdaki gibi listelenmiştir [11]:

- Erişilebilirlik: Servis dışı bırakma (DoS saldırıları), hesap kilitleme, aşırı ara bellek akışı (buffer overflow)
- Veri Güvenliği: Siteler arası komut dosyası çalıştırma (Cross-site scripting), erişim kontrol zayıflıkları, öncelik yükseltme (privilege escalation)

- Ağ Güvenliği: Ağ sızması (network penetration) ve oturum kaçırma (session hijacking)
- Kimlik Yönetimi: Kimlik doğrulama zayıflıkları (IP kaçırma), güvenliksiz güven (farklı kimlik yönetim modelleri farklı güven gereksinimlerine sahiptir)

c) Hizmet olarak Platform (PaaS) Güvenlik Problemleri (Security problems in Platform as a Service-PaaS)

PaaS, altındaki donanım ve yazılım kaynaklarını satın almak ve korumak için bir maliyet gerektirmeden bulut tabanlı uygulamaların dağıtımını kolaylaştırmakta ve böylece müşterilerin uygulamalarını çalıştırıp yönetebileceği bir ortam sunmaktadır [43]. IaaS ve SaaS'da olduğu gibi PaaS de güvenli ve güvenilir bir ağ ve güvenli bir web tarayıcıya bağlıdır. PaaS uygulama güvenliği, PaaS platformunun kendi güvenliği ve bu platform üzerinde dağıtılan müşteri uygulamalarının güvenliği olmak üzere iki yazılım katmanından oluşmaktadır [6]. PaaS sağlayıcıları müşteri uygulamalarını çalıştıran ve çalışma zamanı makinalarını içeren platform yazılım yığınını güvence altına almaktan sorumludur. Diğer modellerde olduğu gibi PaaS'de de aşağıda verilen güvenlik problemleri bulunmaktadır:

Üçüncü parti ilişkileri:

PaaS yalnızca geleneksel programlama dilleri sağlamakla birlikte mashuplar (birbirinden bağımsız web servis sağlayıcı uygulamalarının bir araya getirilerek yeni bir uygulama oluşturulması) gibi üçüncü taraf web hizmetleri bileşenleri de sunmaktadır [6]. Mashuplar, birden fazla kaynak öğesini tek bir entegre birimde birleştirdiği için, PaaS modelleri, veri ve ağ güvenliği gibi mashuplarla ilgili güvenlik sorunlarına da maruz kalmaktadır. Hizmet tabanlı bir mimari olduğundan dolayı ortadaki adam (man in the middle), DoS, XML ile ilişkili saldırılar ve enjeksiyon saldırıları (SQL injection) gibi hizmet tabanlı mimari (SOA-Service-oriented Architecture) ile ilişkili güvenlik sorunları, PaaS'de gerçekleşen en büyük güvenlik problemlerindendir [38]. Ayrıca, PaaS kullanıcıları, web tabanlı geliştirme araçlarının güvenliğine ve üçüncü taraf hizmetlere güvenmek zorundadırlar. Eğer üçüncü taraflar tarafından sağlanan bulut platformu, uygulama geliştirmek için güvensiz bir arayüze izin veriyorsa kötücül bir kod, uygulamaya yerleştirilebilmektedir [7].

Geliştirme yaşam döngüsü:

Uygulama geliştirme perspektifinden bakıldığında, geliştiriciler bulutta barındırabilecek güvenli uygulamalar oluşturma karmaşıklığı ile yüz yüze kalmaktadır. Bulutta uygulamaların değişme hızı, hem sistem geliştirme döngüsünü hem de güvenliğini etkileyecektir. Geliştiriciler, PaaS uygulamalarını sıkça yükseltmeleri (upgrade) gerektiği için, uygulama geliştirme süreçlerinin değişikliklerini takip edebilecek kadar uygulamalarının esnek olmasını sağlamalıdır [44]. Bununla birlikte, PaaS bileşenler üzerindeki yapılandırma ve ayarlar kritiktir. Bir saldırgan tarafından yapılan ayarlardaki değişimler ya da modifikasyonlar bulutun tamamını etkileyebilmekte, geliştirici uygulamalarının güvenliğini tehlikeye atabilmektedir [38]. Güvenli geliştirme tekniklerinin yanı sıra, verilerin uygun olmayan yerlerde depolanmasını önlemek için, geliştiricilerin hukuki konularında da eğitim almaları gerekmektedir. Veriler, veri mahremiyetini ve veri güvenliğini tehlikeye atabilecek farklı yasal rejimlerle farklı yerlerde saklanabilir [6].

PaaS altında yatan altyapı güvenliği:

PaaS'de geliştiricilerin alt katmanlara erişim yetkisi olmadığı için, altta yatan bulut alt yapısı üzerinde kontrol sağlamamakta, yalnızca buluta taşınan uygulamalar üzerinde bir güvenlik kontrolü sağlanmaktadır [43]. Sadece sağlayıcılar, altyapıyı ve uygulama servislerini güvence altına almaktan sorumludur [16]. Bu yüzden geliştiriciler, uygulamalarının güvenliğini kontrol altında tutsalar bile, bir PaaS sağlayıcı tarafından sunulan geliştirme ortamı araçlarının güvende olduğuna emin olamamaktadır.

d) Hizmet olarak Altyapı (IaaS) Güvenlik Problemleri (Security problems in Infrastructure as a Service-IaaS)

IaaS, internet üzerinden erişilebilen sanallaştırılmış bir sistem olarak sunucular, depolama birimleri, ağlar ve diğer hesaplama kaynakları gibi bir kaynak havuzu sağlamaktadır. Kullanıcılar kendilerine tahsis edilen kaynaklar üzerinde tam kontrol ve yönetim sağlayarak herhangi bir yazılımı çalıştırmaya yetkilidirler [4]. IaaS üzerinde bulut kullanıcıları; sanal

makine monitöründe güvenlik açığı olmadığı sürece diğer modeller ile karşılaştırıldığında güvenliği daha iyi kontrol altına alma hakkına sahiptirler [4]. Yazılımlarını sanal makineler üzerinde çalıştırabilirler. Ayrıca güvenlik poliçelerinin doğru yapılandırılmasından kullanıcılar sorumludur, fakat altta yatan hesaplama, ağ ve depolama altyapısı bulut sağlayıcılar tarafından kontrol edilmektedir. IaaS sağlayıcıları oluşturma, iletişim, izleme, değiştirme ve hareketlilikten (mobility) kaynaklanan tehditleri minimize etmek için sistemlerini güvenlik altına almaya büyük çaba göstermelidirler. IaaS modeline dayanan bazı güvenlik problemleri genellikle sanallaştırma ile ilgili olup aşağıda listelenmiştir:

Sanallaştırma:
Kullanıcıların bilgisayar kaynaklarını sanallaştırarak (ağ, CPU, hafıza ve depolama vb.) sanal makineleri yaratmasına, kopyalamasına, paylaşmasına ve geri almasına olanak tanımakta ve bu da tek bir donanım üzerinde birden fazla bağımsız sistemin çalıştırılmasına imkan sağlamaktadır [45]. Fakat sanallaştırma ile birlikte güvenlik altına alınması gereken yeni bir katman eklendiği için saldırganlar bu katmanı kullanarak sistemlere sızabilmektedirler [18]. Bu yüzden sanal makine güvenliği, fiziksel makine güvenliği kadar önem kazanmakta ve her iki kusur birbirini etkilemektedir. Sanallaştırılmış ortamlar da normal altyapılara yönelik her türlü saldırıya karşı savunmasızdır. Bununla birlikte, sanallaştırma ile daha fazla giriş noktası ve daha fazla ara bağlantı karmaşıklığı oluşturduğundan dolayı güvenliği sağlamak büyük bir sorun haline gelmektedir [18].

Sanal makine monitörü:
Sanal Makine Monitörü (Virtual Machines Monitor - VMM) veya sanal makine izolasyonundan sorumlu olan hipervizör, sanal makineyi (virtual machine-VM) başlatma, kapatma, durdurma gibi kontrol hareketlerini ve VM kaynaklarındaki değişiklikleri yönetmektedir [45]. Bu nedenle, VMM ele geçirilirse, sanal makineler de tehlikeye düşebilmektedir. VMM, sanal makineleri kontrol eden ve izleyen düşük seviyeli bir yazılım olduğu için herhangi bir geleneksel yazılım güvenlik kusurlarını içerisinde barındırabilmektedir [10]. Ayrıca hipervizörü yöneten sistem yöneticisi veya ayrıcalığa sahip herhangi yetkilendirilmiş bir kullanıcı, arka planda kontrolü ele geçirerek bu prosedürü kötüye kullanabilmektedir [45]. VMM'i olabildiğince basit ve küçük tutmak, güvenlik açığı riskini azalttığı için zayıflıkları bulmak ve düzeltmek daha kolay olacaktır.

Paylaşılmış kaynaklar:
Aynı sunucudaki VM'ler CPU, bellek, I/O ve diğer kaynakları (sabit sürücü, ağ birimi vs.) paylaşabilmektedir. VM'ler arasındaki kaynakları paylaşmak, her bir VM'nin güvenliğini azaltabilir. Örneğin, kötü amaçlı bir VM, diğer VM'ler hakkındaki bazı bilgileri hipervizörden ödün vermeden paylaşılan bellek veya diğer paylaşılan kaynaklar yoluyla çıkarabilmektedir [19]. Gizli kanalları kullanan iki VM, VMM güvenlik modülü tarafından tanımlanan tüm kurallara uymadan iletişim kurabilmektedir [6]. Böylece, kötü amaçlı bir VM, paylaşılan kaynakları kendi VMM'leri tarafından fark edilmeden izleyebilir; dolayısıyla saldırgan diğer VM'ler hakkında bazı bilgilere ulaşabilir.

Açık sanal makine (VM) görüntü deposu:
IaaS ortamlarında, VM görüntüsü, VM'ler oluşturmak için kullanılan yapılandırma dosyalarını içeren önceden paketlenmiş bir yazılım şablonudur [6]. Dolayısıyla, bu görüntüler bulutun genel güvenliği için bir temel teşkil etmektedir. Kötücül bir kullanıcı sıfırdan kendi VM imajını oluşturabilir, sağlayıcı deposunda saklanan herhangi bir görüntüyü kullanabilir veya VM oluşumu sırasında bir VM imajı çoğaltılarak içerisine kötücül bir kod enjekte edebilir [7]. Örneğin, Amazon, meşru kullanıcılarına bir VM görüntüsü indirebilecekleri veya yükleyebilecekleri bir ortak görüntü deposu sunmaktadır. Kötü amaçlı kullanıcılar, kötü niyetli kodları içeren görüntüleri diğer kullanıcılara veya hatta bulut sistemine zarar verecek şekilde kamuya açık depolarda saklayabilir.

Sanal makine (VM) göçü ve geriye dönüştürme:
Aktif bir VM bir fiziksel makineden başka bir fiziksel makineye aktarılırken VM dosyalarının içeriği çeşitli saldırılara karşı savunmasız kalabilmektedir. Örneğin, geri alma işleminin uygulanması için korunan çalışma durumu günlüğü, VM göçü sırasında erişilebilir hale gelebilmektedir [7]. Bir VM'in geriye dönüştürülmesi, VM'de bir hata oluştuğu durumlarda gerçekleşmektedir ve VM'ler

hatadan önceki durumlarına geri döndürülebilmektedir. Ancak VM geri alma işlemi, makineleri daha önce devre dışı bırakılmış hesapların veya parolaların geri döndürülmesine veya yeniden etkinleştirilen güvenlik açıklarına maruz bırakabilmektedir [6]. Geri almaları sağlamak için, sanal makinenin bir "kopyası" (snapshot) alınmalıdır; bu da yapılandırma hatalarının ve diğer güvenlik açıklarının çoğalmasına neden olabilir.

Sanal ağlar:
Bulut sağlayıcılar, verilerini sıkıştırarak ya da ağ bileşenleri ve diğer kaynakları farklı kiracılar arasında paylaştırarak minimize etmektedir [40]. Daha önce de belirtildiği gibi paylaşım kaynakları, saldırganların çapraz kullanıcı saldırısı başlatmalarına izin vermektedir. Saldırganlar, VM'lerdeki kötücül programlar arasında veri alışverişinde bulunmak için VM'ler ve ana makine arasında veri aktarımına izin veren paylaşılan bir kaynak üzerinden bazı yararlı özellikleri istismar edebilirler [45]. Sanal ağlar, bulut bilişimde önemli bir güvenlik tehlikesi olan VM'lerin birbirine bağlanmasını artırmaktadır. En güvenli yol, özel VM'leri kullanarak her bir VM'i ana bilgisayarıyla bağlamaktır [45]. Bununla birlikte birçok denetleyici, sanal ağları doğrudan ve etkili bir şekilde iletişim kurmak amacıyla VM'leri bağlamak için kullanır. Örneğin, Xen gibi çoğu sanallaştırma platformu, sanal ağları yapılandırmak için köprülü ve yönlendirilmiş olmak üzere iki yol sunmaktadır [6]. Ancak bu teknikler, sanal ağı dinleme ve taklit etme gibi bazı saldırıların yapılma olasılığını artırmaktadır.

e) Bulut Platforma Karşı Yapılan Saldırılar (Attacks against Cloud Platform)
Bir bulut platformu, kendi hizmet teslim modelini kullanarak birçok hizmet sunmaktadır. Fakat bulut platform üzerindeki saldırılar, hizmet kalitesine zarar vermek ve veri korumasını ihlal etmek için bulut hizmet modelinin her katmanında çeşitli bileşenleri istismar etmektedir [7]. Bu bölümde bulut üzerinde meydana gelen saldırılar ve saldırıların yapıldığı bulut platform katmanları hakkında bilgi verilerek 17 farklı saldırı yöntemi incelenmiştir.

Hizmet hırsızlığı:
Bu saldırıda, bir sistem değişkenlerini sıfırlayarak (işlemci zamanı, hafıza sınırı ve vb. diğer değişkenler) daha az ödeme ile sanal makineyi daha uzun süre kullanmasına izin verir [46]. Saldırı, zayıf olan sanal makineler tarafından CPU kullanımını tespit edemeyen veya hesaba katmayan bir zamanlama mekanizması kullanıldığında gerçekleşir [8].

Hizmet aksatma:
Bu saldırı türünde saldırgan bulut platformunu hedef alarak bulut müşterilerine sağlanan hizmetlerin kullanımını engellemektedir [47]. Çoğu senaryoda kurban sistemin bant genişliği veya kaynakları, web sunucular, CPU, Depolama ve diğer ağ kaynakları hedef olarak alınmaktadır [47]. İçerideki kötücül bir kullanıcının kaynakları işgal ederek diğer kullanıcılardan gelen isteklere cevap verilmemesini sağlaması, bu saldırı yöntemi ile yapılmaktadır [7]. Bulut platformunda özellikle XML tabanlı dağıtık hizmet aksatma (DDoS) [70] ve HTTP tabanlı DDoS [69] [70], geleneksel hizmet aksatma saldırılarına göre daha yıkıcı olmaktadır. Çünkü HTTP ve XML, bulut bilişimin kritik ve önemli elemanları olmalarına rağmen bu protokolleri korumak için güçlü bir mekanizma geliştirilmemektedir. Bu yüzden bu protokoller üzerinden güvenliği sağlamak bulut platformunun sağlıklı bir şekilde geliştirilmesinde çok önemli bir rol oynamaktadır [8].

Veri temizleme:
Veri temizleme saldırısında kullanıcı, kendisine ait veriyi bulut deposundan silerken dosya sistemleri veriyi tamamen yok etmemektedir. Bunun sonucunda silinen veri, saldırganlar tarafından yeniden geri kazanılabilmektedir [7].

Müşteri veri manipülasyonu:
Bulut platformuna dışardan erişim sağlayan herhangi bir kullanıcı, uygulama bileşeninden sunucu uygulamasına gönderilen verileri değiştirerek web uygulamalarına saldırabilmektedir. SQL enjeksiyonu, komut enjeksiyonu ve siteler arası betik çalıştırma saldırıları ile veri manipülasyonu gerçekleştirilebilmektedir [6].

Veri sızıntısı:
Verinin transferi, depolanması, denetimi ve işlenmesi sırasında veri sahibinin yetki verdiği kullanıcılar dışında farklı kişiler tarafından ele geçirilmesi işlemine veri sızıntısı denilmektedir [2]. Veri sızıntısı riski, büyük şirketlerde sağlam

ve katı bir güvenlik politikasına sahip olmayan kişisel cihazlarını kullanan çalışan sayısı arttıkça artma ihtimali yüksektir. Çalışanlar bu cihazları evden veya başka bir ortamdan depolama hizmetlerine (Dropbox veya OneDrive gibi) erişmek için kullandıklarında, özellikle işletim sistemlerinin eski sürümleri kullanıldığında güvenlik ihlali riski artmaktadır. Bu potansiyel risk, şirket tarafından sağlanan BT cihazları tarafından da tamamen sonlandırılamamaktadır. Çünkü güvenli olmayan ağlara bağlantılar, kolayca veri sızıntısına yol açabilmektedir.

Buluta kötücül yazılım enjekte etme:
Bulut enjekte edilen kötücül yazılım aracılığı ile bulut verileri ele geçirilip değiştirilebilmekte ve verilere erişim engellenebilir hatta veri üzerinde istenilen tüm haklara sahip olunabilmektedir. Bu saldırıda düşman kendi kötücül hizmet uygulama modelini (SaaS ya da PaaS) ya da sanal makine örneğini (IaaS) oluşturur ve buluta ekler [34]. Daha sonra bu sistemlerin düşman tarafından saldırıya uğramış bazı özel hizmetler için geçerli örnekler arasında olduğunu ve bazı yeni hizmet uygulama örnekleri olduğunu bulut sistemine inandırır. Eğer bu davranış başarılı olursa bulut otomatik olarak geçerli kullanıcının isteklerini kötücül hizmet uygulamasına yönlendirir ve kötücül kod çalıştırılır [34].

Çapraz-VM yan kanallar:
VM taraflı kanal saldırısı, kurban bir VM'i kullanarak saldırganın VM dönüşümünü gerçekleştirdiği ve kurbanın davranışını çıkarmak için işlemci kasalarını güçlendirdiği erişim odaklı bir saldırı yöntemidir [8]. Bu saldırı, kurbanın sanal makinesini kullanarak aynı fiziksel donanım üzerinde saldırganın farklı bir VM üzerinde bulunmasını gerektirmektedir [8]. Güvenlikle ilgili hassas bilgileri türetmek veya sızdırmak için bir sistemde düşük bant genişliğini sonuna kadar kullanan Çapraz-VM yan kanal saldırısı modern bilgisayar sistemlerine yönelik gerçekçi bir tehdit olarak kanıtlanmıştır [48].

VM kaçışı:
VM kaçışı, kötü niyetli bir kullanıcının veya sanal makinenin, sanal makine monitörü (VMM) ya da hipervizörün kontrolünden kurtulduğu durumdur. Bu saldırı ile tüm sanal makinelerin yönetildiği ve erişimlerinin donanıma bağlandığı bir yazılım bileşeni olan VMM çökertilebilir ya da diğer sanal makinelere erişim sağlanabilmektedir [35].

VM atlama:
Bir sanal makinenin diğer bir sanal makinenin zafiyetinden yararlanarak bu makineyi istismar etmesi ve makineye erişim sağlamasıyla yapılan saldırıdır [6]. Bu durum aynı ana bilgisayar üzerinde çalışan VM'ler üzerinde gerçekleşebilmektedir [65]. Saldırgan bu saldırı yöntemi ile IP numarası bilinen bir VM'in trafiğini gözlemleyerek trafik akışını değiştirebilir, manipüle edebilir veya konfigürasyon dosyasını değiştirerek sanal makinenin dosyalarını değiştirebilir [65].

Kötücül VM oluşturma:
Bir sanal makine imajı, sanal makine (VM) oluşturmak için kullanılan bir sanal aygıt türüdür ve bu sanal makine imajları, makine için başlangıç dosya sistemi durumunu ve yazılımı içermektedir [49]. Geçerli hesaba sahip olan bir saldırgan, içerisinde Trojan atı gibi kötü amaçlı kod içeren bir sanal makine imajı oluşturabilmekte, diğer kullanıcılar bu imajı kullandıklarında ya da kendi sanal makinelerini oluşturduklarında bu kötücül kod, onlara bulaşabilmektedir [6] [49]. Ayrıca saldırgan, sağlayıcıların depolarında herkese açık olarak saklanan imajlardan gizli verileri de okuyabilmektedir [49].

Güvensiz VM göçü:
Birçok sanal makine arasında donanım paylaşımı yapılırken bazı durumlarda yük dengesini sağlamak veya poliçelere uymak amacı ile sanal makineler, farklı donanım platformları arasında dolaşmaya zorlanmaktadır ve bu olaya VM göçü denilmektedir [50]. Sanal makinelerin canlı göçü, VM durum dosyalarının içeriğini ağa açık hale getirmektedir [6]. Bu durumdan yararlanan saldırgan, göç sırasında veriye yasal olmadan erişebilir, güvensiz bir makineye VM transferi yapabilir, ayrıca karışıklığa ve DoS ataklarına yol açan birçok VM oluşturabilir ve göçünü sağlayabilir [50].

Sanal ağların kandırılması:
VM'lerin güvenliği için her VM'yi özel fiziksel kanalları kullanarak ana bilgisayarına bağlamak maliyetli bir çözüm olduğundan dolayı çoğu hipervizör, VM'leri daha doğrudan ve verimli bir şekilde iletişim kurmak için bağlamak için sanal

ağları kullanmaktadır [6]. Sisteme dahil olan kötücül bir VM, sanal ağı dinleyebilir hatta paketleri diğer VM'lere yönlendirerek ARP kandırma yapabilmektedir. Xen gibi çoğu sanallaştırma platformu, sanal ağları yapılandırmak için köprülü ve yönlendirilmiş olmak üzere iki yöntem kullanmakta, fakat bu yöntemler de sanal ağın kandırılma olasılığını artırmaktadır.

Hedeflenmiş paylaşılan hafıza:
Bu saldırı türünde saldırganlar hem fiziksel hem de sanal makinelerin paylaşılmış hafızalarından yararlanarak, çalışan işlem sayısı, belirli bir süre içerisinde oturum açan kullanıcı sayısı ve hafızada bulunan geçici çerezler gibi bulutun iç yapısını ortaya çıkaran bilgilere yetkisiz erişim sağlayabilirler [8]. Geçerli kullanıcının paylaşılan hafızaya erişimini kısıtlayan mevcut anti virüsler veya güvenlik duvarları dışında bu saldırıyı önleyen güçlü bir çözüm, literatürde ve pratikte bulunmamaktadır.

Kimlik avı:
Kimlik avı saldırısı, kişisel bilgilere yetkisiz olarak erişilmesine, kullanıcı bilgisayarına kötücül bir kod indirilmesine, bulut bilişim yapısının normalden farklı bir şekilde davranmaya zorlanmasına ve son kullanıcı için sunucunun erişilemez olmasına yol açmaktadır [8] [51]. Ayrıca bu saldırı sadece kullanıcılar üzerinde değil, aynı zamanda elektronik bankalar ve elektronik ödeme sistemleri gibi destekleyici finansal kurumları da savunmasız hale getirebilmektedir [51].

Botnetler:
Açık bir bulut ortamı göz önüne alındığında, yönlendirme ve şaşırtma açısından uzaktan yönetilen zombi bilgisayarların en tehlikeli gruplarından biri olan botnetler aracılığıyla bulut kaynaklarına yetkisiz erişim yapılabilmektedir. Ayrıca bulut sisteminin anormal bir şekilde çalışması sağlanabilmekte, hassas bilgiler ve kullanıcı verileri çalınmaktadır [52]. Teknoloji geliştikçe botnetlerin ağlardaki kamuflajını anlamak zorlaşmakta ve yeni nesillerinde algılanması için kendilerini ağ içerisinde nasıl gizlediğini öğrenmek gerekmektedir.

Sesli Steganografi:
Bulut depolama sistemlerinin en tehlikeli saldırılarından biri olan bu saldırısı ile kullanıcıların düzenli olarak ses dosyalarında sakladıkları gizli veriler istismar edilebilmektedir [8]. Bir kullanıcı, gizli verisini normal bir ses dosyası gibi bir medya dosyası içerisine saklayarak gönderebilmekte, bu durumdan yararlanan saldırganlar, kendi kötü amaçlı kodlarını ses dosyalarında saklayıp kurban sunuculara göndererek bulut sistemlerini korumak için alınan geleneksel önlemler ve mevcut güvenlik mekanizmalarını aldatmaktadırlar [68].

VM geri alma:
Zafiyeti en fazla alan olan sanallaştırma ortamına yapılan diğer saldırılardan biri olan VM geri alma saldırısında bir hipervizör, çalışma sırasında herhangi bir zamanda bir VM'i askıya alabilir, mevcut CPU durumlarının, disk ve hafızanın anlık görüntüsünü alabilir ve ziyaretçi VM farkındalığı olmadan daha sonra anlık görüntüsünü almaya devam edebilmektedir [36]. Bir geri alma saldırısında saldırgan, önceki anlık görüntülerden yararlanabilir ve kullanıcının farkındalığı olmadan makineyi çalıştırıp daha sonra geçmişini temizleyebilir. Bu şekilde aynı veya farklı bir anlık görüntüyü tekrar tekrar çalıştırabilir. Bu şekilde saldırgan, geçmişini temizleyerek yaptığı şüpheli davranışlardan dolayı yakalanmamaktadır [36]. Bu makalede açıklanan saldırı gruplarının adı, her grupta bilinen saldırı olayları, bu saldırılara sebep olan istismar edilebilir zafiyetler, bulut bilişim modelinde saldırıların uygulandığı katman ve saldırının meydana getirdiği sonuçların genel bir özeti Tablo 3'de verilmiştir.

IV. LİTERATÜRDE ÖNERİLEN ÇÖZÜMLER (PROPOSED SOLUTIONS IN LITERATURE)

a) Hesap ya da hizmet hırsızlığı tehdidine karşı önlemler (Countermeasures against account or service hijacking)

Kimlik ve erişim yönetimi rehberliği:
Bulut Güvenlik Birliği (Cloud Security Alliance) tarafından yayınlanan rapor, hizmet aksatma tehdidine karşı merkezi dizin, erişim yönetimi, kimlik yönetimi, rol tabanlı erişim kontrolü, kullanıcı erişim sertifikasyonları, ayrıcalıklı kullanıcı ve erişim yönetimi, görev ayrımı, kimlik ve erişim raporlaması olmak üzere birçok önlem içermektedir.

Tablo 3. Bulut Bilişimin Maruz Kaldığı Saldırılar (Attacks on cloud computing) [6] [8] [14]

Saldırı	Saldırı olayları	Zafiyet	Kategori	Sonuçları
Hizmet hırsızlığı	○ Sanal makineye saldırı [46]	▪ Güvenlik standardı ve denetim yokluğu ▪ Ağ güvenlik duvarının uygun olmayan kurulumu ▪ İnternet protokol zafiyetleri ▪ Kötücül içerideki kullanıcılar ▪ Tarayıcı güvenliği ▪ Hatalı güvenlik yapılandırması	SaaS IaaS	➢ Faturalandırma olmadan bulut hizmeti kullanımı ➢ Bulut kaynaklarının çok az maliyetle veya maliyetsiz çalınması
Hizmet aksatma	○ DDoS (Dağıtık Dos) [47] ○ Http tabanlı DDos [69] [70] ○ XML tabanlı DDos [70] ○ REST tabanlı DDos [71]	▪ Güvenlik standardı ve denetim yokluğu ▪ Hesap ve hizmet kaçırma ▪ Tarayıcı güvenliği ▪ Hatalı güvenlik yapılandırması ▪ Sınırsız kaynak ayrımı [14]	SaaS IaaS	➢ Hizmet/ donanım aksaklığı ➢ Bilgi için yetkisiz erişimi elde etmek amacıyla XML imzasına kötücül kod yerleştirme ➢ Güvensiz Http tarama üzerinden tarayıcı geçmişine ya da herhangi özel bir bilgiye erişme
Veri temizleme	○ Veri koruma ihlali [60]	▪ Bilinmeyen sahipler tarafından verinin yerleştirilmesi ▪ Tamamlanmamış veri silme-verinin tamamen silinememesi	SaaS PaaS IaaS	➢ Silinen verinin saldırganlar tarafından geri kazanılması
Müşteri veri manipülasyonu	○ SQLve komut enjeksiyonu [60] [61] ○ Siteler arası betik çalıştırma [6] [60]	▪ Güvensiz arayüzler ve API'ler	SaaS	➢ Web uygulamalarına yetkisiz erişim
Veri sızıntısı	○ Veri sahibinin yetki verdiği kullanıcılar dışında farklı kişiler tarafından ele geçirilmesi [2] [60]	▪ Bilinmeyen sahipler tarafından verinin yerleştirilmesi ▪ Tamamlanmamış veri silme-verinin tamamen silinememesi ▪ Güvenilir olmayan üçüncü taraf sağlayıcısı tarafından veri yedekleme ▪ Verinin şifresiz bir şekilde saklanması, işlenmesi ve iletilmesi ▪ Sanal makine ve sanal ağlarda oluşan zafiyetler	SaaS PaaS IaaS	➢ Verinin kötüye kullanımı ➢ Veri gizliliği ihlali
Kötü amaçlı yazılım enjeksiyonu	○ Buluta kötücül yazılım enjekte etme [8] [62]	▪ Teknik kusurların paylaşımı ▪ Kötücül içerideki kullanıcılar ▪ Öncelikli kullanıcı erişimi ▪ API'nin güvensiz altyapısı	IaaS	➢ Kimlik bilgilerinin sızılması ➢ Kullanıcı verisinin sızıntısı ➢ Bulut makinenin anormal davranışı
Çapraz VM yan-kanal	○ Zamanlama yan-kanal [63] ○ Enerji tüketimi yan-kanal [64]	▪ API'nin güvensiz arayüzü ▪ Hatalı güvenlik yapılandırması	IaaS	➢ Kullanıcı veri/bilgi sızıntısı ➢ Bulut kaynakları/altyapı bilgi sızıntısı
VM kaçışı	○ Sanal makinenin kontrolsüz kullanımı [35] [65]	▪ Karmaşık hipervizör kodu ▪ VM'ler ya da hipervizörlerin esnek konfigürasyonu	IaaS	➢ Hipervizörlerin işlevsiz hale getirilmesi ➢ Sanal makinelere yetkisiz erişim sağlanması
VM atlama	○ Sanal makinenin istismar edilmesi [65]	▪ VM'ler ile sınırsız kaynak ayırma ve kaldırma ▪ VM'ler ya da hipervizörlerin esnek konfigürasyonu	IaaS	➢ Aynı ana bilgisayar üzerindeki birçok sanal makineye yetkisiz erişim

Kötücül VM oluşturma	○ Sanal makine imajlarına kötücül kod bulaştırma [49]	▪ Genel depolarda VM imajlarının kontrolsuz yer değişimi ▪ VM imajları hareketsiz halde oldukları için yama yapılamamaktadır.	IaaS	➢ Herkese açık olarak saklanan imajlardan gizli verilerin okunması ➢ Bulut sisteminin anormal çalışması
Güvensiz VM göçü	○ DoS ataklarına yol açan birçok VM oluşturma ve göçünü sağlama [50]	▪ VM'lerin IP adresleri bulutta herhangi birine görünür haldedir. Saldırganlar bulutta hedef VM'in bulunduğu yeri tespit edebilmektedir.	IaaS	➢ Göç sırasında veriye yasal olmadan erişim ➢ Güvensiz bir makineye VM transferi
Sanal ağların kandırılması	○ Sanal ağın dinlenmesi [19] ○ ARP kandırma [66]	▪ Çeşitli sanal makineler tarafından sanal köprülerin paylaşımı	IaaS	➢ Veri gizliliği ihlali
Hedeflenmiş paylaşılan hafıza	○ Kötücül kod enjeksiyonu saldırısı ile sanal makinelerdeki bellek yığınlarına erişim [67]	▪ Güvenlik standardı ve denetim yokluğu ▪ Hesap ve hizmet kaçırma ▪ API'nin güvensiz arayüzü ▪ Hatalı güvenlik yapılandırması	IaaS	➢ Bulut kaynaklarından bilgi sızıntısı ➢ Kullanıcı bilgi/veri sızıntısı ➢ Yan kanallar ve buluta kötü amaçlı yazılım enjeksiyonu gibi diğer saldırılar için açık pencere sağlar
Kimlik avı	○ Hesap ve hizmet hırsızlığı [46] [51]	▪ Güvenlik standardı yokluğu ▪ Ağ güvenlik duvarının uygun kurulumu ▪ İnternet güvenlik zayıflıkları ▪ Hesap ve hizmet kaçırma ▪ Kimlik doğrulama mekanizması ▪ Tarayıcı güvenliği	SaaS PaaS IaaS	➢ Kişisel bilgilere yetkisiz erişim ➢ Kullanıcı bilgisyarına zararlı yazılım içeren kod kurma ➢ Bulut bilişim yapısını anormal davranmaya zorlama
Botnetler	○ Stepping stone saldırısı [8]	▪ Güvenlik standardı ve denetim yokluğu ▪ Ağ güvenlik duvarının uygun kurulumu ▪ Hesap ve hizmet kaçırma ▪ Kimlik doğrulama mekanizması ▪ Tarayıcı güvenliği	SaaS PaaS IaaS	➢ Bulut kaynaklarına yetkisiz erişim ➢ Bulut sisteminin anormal çalışmasını sağlama ➢ Hassas bilgi hırsızılığı ➢ Kullanıcı verilerini çalma
Sesli Steganografi	○ Kötücül kodların ses dosyası gibi medya dosyalarına yerleştirilmesi [68]	▪ Güvenlik standardı ve denetim yokluğu ▪ Ağ güvenlik duvarının uygun kurulumu ▪ Hesap ve hizmet kaçırma ▪ Tarayıcı güvenliği ▪ Hatalı güvenlik yapılandırması	IaaS	➢ Bulut depolama sistemine erişilememesi ➢ Kullanıcı verisine erişim ➢ Kullanıcı verisinin silinmesi
VM geri alma	○ Kullanıcı farkındalığı olmaksızın makinesinin çalıştırılıp işlemler yapılması ve delillerin bulunduğu geçmişin silinebilmesi [36]	▪ Güvenlik standardı ve denetim yokluğu ▪ Ağ güvenlik duvarının uygun kurulumu ▪ Hesap ve hizmet kaçırma ▪ Tarayıcı güvenliği ▪ Hatalı güvenlik yapılandırması	IaaS	➢ Kaba kuvvet saldırısı başlatma ➢ Bulut altyapısına zarar verme ➢ Hassas bilginin sızması

Tirumala ve arkadaşları [30] temel olarak The New York Times çevrimiçi gazetesinde meydana gelen bulut güvenlik olayının analizi üzerinden yola çıkarak hesap kaçırma saldırısını önlemek ve geçerli olmayan bir kullanıcı tarafından herhangi bir bilgi teknolojisi kaynağına erişimi engellemek için kullanıcı kimlik bilgileri üzerinde tam kontrolün sağlanması gerektiğini savunmuşlardır. Bir şifrenin sıfırlanması için bir talepte bulunulduğunda kullanıcı kimliğinin birden fazla yöntemle doğrulanması (çok faktörlü kimlik doğrulama) sağlanmalı ve eğer şifre, ağ yöneticisi tarafından sıfırlanırsa kullanıcı ilk kullanımdan sonra şifresini değiştirmeli ve her 90 günde şifresini yenilemeli, kullanıcı erişim politika ve prosedürleri kullanıcı ayrıcalıklarına dayalı olarak BT kaynaklarından herhangi birine kullanıcı erişimini sağlamak veya iptal etmek için uygun ve tam olarak belgelendirilmesi, yetkilendirilmesi ve uygulanması önerilmiştir.

Dinamik kimlik bilgileri:
Mobil bulut bilişimde dinamik kimlik bilgisi oluşturmak için sunulan bir algoritma [20] ile kullanıcı pozisyonunu değiştirdiğinde ya da veri paketlerinin sayısını değiştirdiğinde dinamik kimlik bilgilerinin değeri değişmektedir.

Kullanıcı erişim poliçesi değişimleri:
Kullanıcıların sisteme erişim izinleri, işletme gereksinimlerine uygun olmalı ve servis seviyesi sözleşmesinde (Service Level Agreement-SLA) belirtilen kurallara uyulmalıdır. Herhangi bir işletme seviyesinde uygulama verilerine, veritabanlarına ve ağ yapılandırmalarına ilişkin bilgilere erişim izni verilmeden önce kimlik bilgileri doğrulanmalı, kritik verilere erişim isteğinde ise kullanıcı izinleri kısıtlanmalıdır [30]. İşletmeye yeni iş ortaklarının dahil edilmesi, yeni müşterilerle yapılan sözleşmeler / anlaşmalar, eski müşterilere yapılan hizmet değişiklikleri, çalışanların yerinin değiştirilmesi veya sonlandırılması vs. durumlarda örgütsel sistemlere kullanıcı erişimi zamanında sağlanmalı, geçerli olmayan kullanıcıların erişimi iptal edilmelidir [30].

Bununla birlikte sisteme yetkili ya da yetkisiz girişler dahil olmak üzere sistem içerisinde yapılan tüm aktivitelerin, sistem istisnaları ve güvenlik olayları ile ilgili bilgilerin bilgi güvenliği politikaları ve düzenlemelerine uygun olarak saklanması gerektiği belirtilmektedir. Ayrıca tutulan bu kayıtların yer aldığı denetim kayıt bilgilerinin günlük olarak gözden geçirilmesi ve denetim günlüğü bilgilerine erişimin küçük bir güvenilir personel grubuyla sınırlı tutulması gerekmektedir.

Tek kullanımlık şifreler (one time password) ve belirteç tabanlı kimlik doğrulama (token based authentication):
Bulut sistemini sağlayan işletmeler bilinçlendirme programları uygulayarak müşterilerini ve satıcılarını eğitmelidir. Ayrıca web uygulamaları güvence altına alınmalı ve kullanıcı, kimlik bilgilerini kullanarak giriş yapması gerektiğinde, tek kullanımlık PIN numarasını mobil cihazına girmesi ve bu numaranın otomatikleştirilmesi için bir belirteç tabanlı kimlik doğrulaması yapılmalıdır. Kullanıcılar, hesaplarına yalnızca bu PIN numarasını kimlik bilgileriyle birlikte girdiklerinde erişebilmelidir [74].

b) Hizmet aksatma (DoS-DDoS) saldırısına karşı önlemler (Countermeasures against denial of service (DoS-DDoS) attacks)

Iyengar ve Ganapath [90] tarafından DDos saldırılarına karşı Kaotik Teori kullanarak *Ağ trafik analizi*, *Anomali tespiti* ve talep sahiplerinin özelliklerini doğrulamak için *Aşırı yük sınıflandırması* olmak üzere üç modülden oluşan bir mekanizma önerilmiştir. İstek sahibinin talep ettiği trafik, kararlılık durumunun belirlendiği Ağ Trafiği Analizi aşamasını her zaman atlamaktadır. Trafik kararlılık durumu sezgisel yöntemlere dayalı olarak türetilmektedir. Ağ trafiği, önerilen dinamik trafik sistemi için Lyapunov'un kararlılık teorisini dikkate alan bir anomali tespit modülüne izin vermektedir. Lyapunov'un kararlılık teoremi, denge durumuna yakın olan çözümlerin kararlılık durumunun bulunduğu noktayı belirtmektedir. Kararlılık durumuna ve belirsiz trafik koşulunun olasılık ölçüsüne dayanarak, aşırı yük durumu normal veya anormal olarak tahmin edilmektedir. Daha sonra aşırı yüklenme nedeni kesin olarak tahmin edilmekte ve saldırı örnekleri filtrelenirken saldırı olmayan durumlarda veri merkezi kaynaklarına erişilmesine izin verilmektedir.

Gupta ve arkadaşları [75], DDos saldırılarına karşı alınan koruma önlemleri *Önleme*, *Tespit* ve *Karşılık verme* olarak üç grupta değerlendirmiştir. Önleme mekanizmasında,

kurumlar daha çok kendi sistemlerini güvenceye alarak internet güvenlik protokol ağları tarafından geliştirilen politikaları uygulamaktadır. Buna sıkı güvenlik denetimi denilmektedir. Zombiler ya da botlar kullanılarak yapılan DDos saldırıları, sistemlerin botnet olmalarını engelleme, botnet algıları stratejileri geliştirme gibi işlemler ile önlenebilmektedir. Son olarak kaynak doğrulama yöntemi ile ana bilgisayarlar ve yönlendiriciler, saldırının kaynağını doğrulamaya çalışmaktadır. Bu durumda ana bilgisayar bağlantı kurulumunun bot tarafından değil bir insan tarafından yapıldığından emin olmaktadır. Bu mekanizmalar ağ katmanı seviyesinde paketin başlık bilgisini kullanarak paketin güvenilirliğini kontrol edebilmektedir. Uygulama seviyesinde kullanıcıların gerçekliğini doğrulamak için bir CAPTCHA bulmacası ya da metin tabanlı bir soru yönlendirilmektedir. Tespit kategorisinde ise anomali tabanlı ve benzerlik tabanlı olmak üzere iki yöntem önerilmektedir. Son olarak saldırı tespitinden sonra sistemin saldırıyı hafifletmesi veya sonlandırması için paketin kaynağını takip eden *geri izleme (traceback),* eşik değerleri ve saldırı imzalarına dayalı yapılan *filtreleme (saldırı trafiğini hafifletme)* ve yasal olmayan bir trafiği tespit eden *yer paylaşımlı (overlay) ağ* mekanizmaları önerilmektedir.

Darwish ve arkadaşları [76], bulut sistemleri üzerinde yapılan DDos saldırı türlerini IP kandırmaca (IP spoofing), SYN taşırma (SYN flooding), smurf saldırı ve tampon taşma (buffer overflow) şeklinde ayırarak bu saldırılara yönelik savunma mekanizmaları önermişlerdir. IP kandırmaca saldırısına karşı savunma için PaaS katmanında atlama (hop) sayısı filtreleme [77] ve IaaS katmanında güven tabanlı yaklaşımdan [78] bahsedilmektedir. SYN taşırma için ise PaaS katmanında SYN önbellek yaklaşımı, SYN çerezleri savunma yaklaşımı, PaaS katmanında alınan SYN süresinin azaltılması, IaaS katmanında filtreleme ve güvenlik duvarı mekanizması ile birlikte aktif izleme mekanizması önerilmektedir. Smurf saldırısını önlemek için ise PaaS katmanında sanal makineler ve IaaS katmanında ağ kaynakları yapılandırılmaktadır. Son olarak tampon taşma saldırısını önlemek için IaaS katmanında dizi sınır kontrol mekanizmasının uygulanması, statik ve dinamik kod mekanizmalarının analiz edilmesi ve kaynak kod yazımının SaaS katmanında önlenmesi gerektiği vurgulanmaktadır.

a. Müşteri veri manipülasyonuna karşı önlemler (Countermeasures against customer data manipulation)

Web uygulama tarayıcıları:

Bulut altyapısında barındırılacak web uygulamaları, web uygulama tarayıcıları kullanılarak elde edilen zafiyetlerden korunmak için taranmalı ve doğrulanmalıdır [5]. Web uygulamaları çoğunlukla saldırılara açık olduğundan, buradaki güvenlik zafiyetlerini belirlemek için geliştirilen web uygulama tarayıcıları, güvenlik duvarı gibi araçlar web trafiğini yönlendirerek belirli tehditleri denetlemektedir [6]. Bu tür tarayıcılar Ulusal Zafiyet Veritabanı (National Vulnerability Database-NVD) ve Ortak Zayıflık Numaralandırma (Common Weakness Enumeration-CVE)'da muhafaza edilen günümüzde keşfedilmiş güvenlik açıklıkları ve saldırı yollarına paralel olarak güncellenmelidir [5].

Dağıtık Erişim Kontrolü:

Bulut bilişimin çoklu kiracılık ve sanallaştırma özellikleri, yan kanal saldırıları riskini artırarak potansiyel güvenilmeyen kiracılar arasında fiziksel kaynak paylaşımından dolayı bazı erişim kontrolü ve güvenlik zorluklarına yol açmaktadır [53]. Aynı zamanda çoklu kiracılık hesaplamaları girişimi yetkisiz bilgi akışına da yol açmaktadır [53]. Bulut bilişim ortamlarındaki hizmetlerin heterojenliği, erişim kontrol mekanizmalarının tek bir merkezden yönetilmek yerine güvenli ve dağıtık bir bulut altyapısına inşa edilmelerini gerektirmektedir [4] [53]. Merkezi çözümlerde, birden çok bulut alanı üzerinden çok sayıda kullanıcı için erişim kontrolü gerekmekte, çok sayıda yetkilendirme kuralını koruma ile baş edilmektedir [4]. Mevcut çözümler, çoklu otorite kriptografik erişim kontrol modellerini tanımlamaktadır. Bununla birlikte, çoklu erişilebilirlik ve bulut tabanlı dağıtımların doğası ile birlikte daha ölçeklenebilir erişim denetim modelleri geliştirmenin yanı sıra, uygulamaya özel gereksinimleri de göz önüne almak gerekmektedir [4].

Bulutta bir hizmet olarak gizlilik koruma ile veri madenciliği (Privacy-preserving data mining as a service):

Bir hizmet olarak kullanıldığında veri madenciliğine duyulan ilgi giderek artmaktadır [54]. Bu paradigmada, veri depolama, hesaplama kaynakları ve tecrübeli olmayan bir şirket (veri sahibi), verilerini bulutta saklamakta ve madencilik görevlerini bulut hizmeti sağlayıcısına (sunucu) açmaktadır [54]. Bununla birlikte, veri madenciliği aynı zamanda ciddi bir gizlilik sorununu da ortaya koymaktadır; yani sunucu, şirket verilerine erişebilir ve işletme sırlarını öğrenebilir [4]. Bir şirketin veri gizliliğini korumak ve sunucunun buluttaki veriler üzerinde ilişki kuralı incelemesini sağlamak için veri sahibinin, işlem veritabanındaki öğelerin anlamlarını benzersiz sayılarla değiştirerek (sahip olduğu yerlerde) gizliliği sağlayabileceği basit bir çözümü bulunmaktadır [4]. Aynı madde aynı numara ile, farklı maddeler ise farklı numaralar ile ikame edilmektedir. Bu bire bir değiştirme yaklaşımı, öğelerin frekanslarını gizlememektedir. Sunucu, bazı arka plan bilgilerine (örneğin, bazı öğelerin frekanslarıyla ilgili bilgi) sahipse, bu numaları, özellikle en sık kullanılan öğeleri yeniden tanımlayabilmektedir. Veri madenciliği görevlerinin buluta dış kaynak kullanımı paradigmasında şirketin (veri sahibi) veri depolama, hesaplama kaynakları ve uzmanlığından yoksun olduğu varsayılmaktadır [4]. Bununla birlikte, bir veritabanını k destek anonimliği veya k gizliliği olarak değiştirmek, ilişkilendirme kurallarını araştırma algoritmaları kadar karmaşık ve pahalıdır [54]. Eğer şirket sahibi bu yöntemleri kullanabilecek kaynaklara sahip ise, yerel olarak Apriori algoritması gibi ilişkilendirme kuralı madenciliği yürütebilmektedir [54].

Etkin, Ölçeklenebilir ve İnce-Taneli Çözümler:

Güvenilir erişim kontrolü, hassas verilerin gizliliğinin korunarak depolanması için vazgeçilmez bir güvenlik gereksinimidir. Kriptografik erişim kontrol modelleri, bulut tabanlı sistemler için popüler olan güvenli çözümlerdir. İnce taneli erişim kontrol modelleri geliştirmek için kriptografik tekniklerin kombinasyonları kullanılmaktadır. Örneğin bulut için öznitelik tabanlı şifreleme [54], vekil yeniden şifreleme [54], hiyerarşik kimlik tabanlı şifreleme, şifre metni özniteliğine dayalı şifreleme gibi çeşitli kriptografik yöntemler kullanılmaktadır [4].

b. Veri sızıntısına karşı önlemler (Countermeasures against data leakage)

Bölümleme - gereğinden fazla dağıtım yöntemi:

Bu yöntem ilk önce hassas veriyi önemsiz parçalara bölmekte ve böylece herhangi bir parça tek başına önemli bir bilgi bulundurmamaktadır [21]. Daha sonra bu parçalar dağıtık sistemin farklı taraflarında dağıtılmaktadır.

Sayısal imzalar:

Veri internet üzerinden transfer edildiğinde RSA [58], Diffie Hellman anahtar değişimi, AES gibi güçlü algoritmalar ile sayısal imza kullanılarak verinin güvenliği sağlanabilmektedir [57].

Şifreleme:

Şifreleme yöntemleri hassas verinin güvenliği için uzun zamandır kullanılan bir yöntemdir. Bulut içerisinde şifreli verinin depolanması veya verinin şifreli biçimde gönderilmesi, veri güvenliğini garanti altına almaktadır. Fakat kullanılan bu şifreleme yöntemlerinin AES gibi hem hızlı hem de güçlü olması gerekmektedir. Ayrıca Harnik ve arkadaşları [22] tarafından yapılan bir çalışmada şifrelemenin bulut depolama tekilleştirme (deduplication) üzerinde yapılan yan kanal saldırılarını durdurmak için de kullanıldığından bahsedilmektedir.

Homomorfik şifreleme:

Buluta veri gönderilirken standart modelde veri şifrelenip bulut sağlayıcıya gönderildikten sonra veriyi çekmek isteyen kişinin her bir işlem için şifreyi çözmesi gerekmektedir [56]. İstemci gerekli hesaplamaları çalıştırmadan önce bulut sağlayıcıya özel bir anahtar sağlamalıdır ve bu da bulutta depolanmış verilerin gizliliği ve mahremiyetini etkileyebilmektedir [56]. Homomorfik şifreleme ile hesaplamaların şifrelenmiş veriler üzerinde yapılması sağlanmakta [4], ham veri üzerinde direkt olarak yapılan hesaplama sonuçları ile aynı sonuçlar elde edilecek şekilde deşifreleme işlemi olmadan ve herhangi bir özel anahtar bilinmeden şifreli veriler üzerinde çeşitli işlemler yapılabilmektedir [56]. Bu, şifreli verileri buluta dış kaynak olarak sunan bulutlar için büyük bir avantaj olabilir. Homomorfik şifreleme, birçok uygulama için cazip olmasına rağmen ciddi bir kısıtlamaya sahiptir: homomorfik özellik, yalnızca bir

işlemle, genellikle yalnızca toplama veya yalnızca çarpma ile sınırlandırılmıştır [4]. Hem ekleme hem de çarpma için homomorfik özelliklere sahip olan yöntemler, gerçek hayatta olan uygulamalara bir adım daha yaklaşacaktır [4].

Vekil yeniden şifreleme (Proxy re-encryption):
Bu şifreleme yöntemi, bir kullanıcının genel anahtarı kullanılarak şifrelenen verilerin, başka bir kullanıcının özel anahtarı kullanılarak çözülebilecek biçime dönüştürülmesini sağlamaktadır [54]. Fakat yöntem, kullanıcıları veya kimlik niteliklerini ve ilke değişikliklerini ekleme / iptal etme işlemlerini verimli bir şekilde yürütmesini ele almamaktadır [15]. Aynı belgelerin birden çok şifreli kopyasını tutmak gerekmekte ve bu da yüksek hesaplama maliyetlerine neden olmaktadır.

Özellik tabanlı şifreleme (ÖTŞ):
ÖTŞ, iletilerin kullanıcı özniteliklerine göre şifrelenip çözülebildiği açık anahtar şifrelemeye dayalı bir şifreleme ilkesidir [15]. ÖTŞ'de şifreleme anahtarları ya da şifreli metinler sistem kullanıcıları için tanımlayıcı nitelik kümeleri ile etiketlenir ve belirli bir kullanıcı, yalnızca bu özel anahtar ile eşleşen özel bir şifreli metni deşifreleyebilir [55]. Yani şifreli verilere yalnızca anahtarları niteliklerle eşleşen kullanıcılar erişebilir. Öznitelikler, erişim kontrolü politikalarını tanımlamaktadır.

c. Kötücül kod enjeksiyonuna karşı önlemler

Müşteri bulutta bir hesap açtığı zaman sağlayıcı, bulutun imaj depolama sisteminde müşterinin sanal makinesinin bir imajını oluşturmaktadır. Müşterinin çalıştıracağı uygulamalar yüksek verimlilik ve bütünlükle değerlendirilmektedir. Kötücül kod enjeksiyon saldırılarından en yaygın iki saldırı türü, SQL enjeksiyonu ve siteler arası komut dosyası çalıştırma saldırılarıdır.

Zunnurhain ve Vrbsky [62] tarafından yapılan çalışmada bir saldırganın IaaS'ye girmesi (saldırı yapması) zor olduğu için donanım düzeyinde bir bütünlük sağlama önerilerek tüm işletim sistemleri tarafından sanal olarak desteklenen Dosya Tahsis Etme Tablosu (File Allocation Table-FAT) kullanılmaktadır. FAT tablosundan bir müşterinin çalıştıracağı kod veya uygulama hakkında bilgi edinilerek yeni bir örneğin bütünlüğünü ve geçerliliğini belirlemek için müşteri makinesinden daha önce yürütülen önceki örnekler kontrol edilmektedir. Bir başka çalışmada da Zunnurhain ve Vrbsky tarafından önerilen donanımsal çözüme benzer şekilde sağlayıcının sonunda bir Hipervizör dağıtmaya ihtiyaç olduğundan bahsedilmektedir [79]. Bu hipervizör, güvenliğinin hiçbir şekilde ihlal edilemeyeceği bulut sisteminin en güvenli ve en karmaşık kısmı olmalıdır ve müşterinin sanal makinesinin FAT tablosunda yer alan örneğin bütünlüğünü kontrol ederek tüm örneklerin planlanmasından sorumlu tutulması gerekmektedir.

Kötücül kod enjeksiyonunu önlemenin bir başka yolu, orijinal servis örneğinin imaj dosyasında bir şifre (hash) değeri depolamaktır [80]. Böylece orijinal ve yeni hizmet örneğinin görüntüleri arasında bütünlük kontrolü yapılarak kötü amaçlı örneklerin tanımlanması sağlanabilmektedir. Şifre değerleri kullanımının bir sonucu olarak saldırgan bulut sistemini kandırmak ve sistem içerisine kötücül kod enjekte etmek için geçerli bir şifre değeri oluşturmaya ihtiyaç duymaktadır. Bu durum da geçerli değer bulunana kadar sistemin güvende olmasını sağlamaktadır.

d. Çapraz VM yan kanal saldırılarına karşı önlemler (Countermeasures against Cross-VM side channel attacks)

Çapraz VM saldırılarına karşı Kumar ve arkadaşları [33] tarafından önerilen sistemde saldırgan kaba kuvvet (brute force), küçük paket gidiş-dönüş süresi (small packet round trip time) gibi herhangi bir yöntemi kullanarak sunucuyu belirlemeye çalışmakta fakat geliştirilen OpenStack yazılım platformu ile sadece yayın alanının giriş noktasına kadar paketleri izleyebildiği için hedefi saptayamamaktadır. OpenStack; kullanıcıların web tabanlı kontrol paneli, komut satırı araçları ya da Restful API üzerinden yönettiği bir veri merkezi boyunca işleme, depolama ve ağ kaynakları havuzlarını kontrol etmek için API'ler sağlamaktadır.

Yang ve arkadaşları [81] yan kanal saldırılarına karşı sanallaştırma katmanında dört farklı savunma türünden bahsetmektedir. Bunlardan birincisi donanım tabanlı yöntemlerdir. Ancak bu yöntemlerin uygulanması ticari olarak bulutlarda

dağıtılmadan önce güç tüketimi ve ekonomik fizibilite gerektirdiğinden, ayrıca genişletilebilirlik ve esneklik gibi birçok faktör içerdiğinden dolayı sistemi karmaşık bir hale getirdiği belirtilmektedir. İkinci ve üçüncü savunma türü olarak istemcinin ziyaretçi işletim sistemi içerisinde çalışan savunmalar (örneğin korunmuş süreçler için L1 ve L2 önbelleklerine gürültü enjekte edilmesi) veya kriptografik bir anahtarı birden fazla parçaya bölme ve bunları çoklu VM'ler arasında dağıtma gibi uygulama düzeyinde savunmalar bulunmaktadır. Son olarak bulutun rutin işlevleri üzerinde etkisi olabilecek VM'leri olabildiğince izole etmek için paylaşılmış kaynakların istatistiksel çoklanması, program yürütme zamanını gizleme ve harici bir gözlemciye maruz kalan zamanlamayı değiştirmek gibi özellikleri içeren hipervizör tabanlı yaklaşımlar önerilmektedir. Fakat izolasyon tabanlı çözümlerin bellek sayfası (memory-page) ya da CPU önbellek paylaşımını olumsuz olarak etkilediği, bu durumun da kaynakların yetersiz kullanımına sebep olarak bulut bilişimin getirdiği faydaları azalttığı vurgulanmaktadır.

Azab ve arkadaşları [82] literatürde önerilen çözümlerin donanım, istemci sanal makineleri ya da hipervizörler gibi yapılarda önemli değişimler gerektirdiği ve saldırı çeşitlerine özel geliştirilmiş yöntemler olduğunu öne sürerek bu çözümlerin genel olmadığını ve saldırının mutasyona uğramış sürümleri ile başa çıkılamayacağını belirtmiştir. Bu yüzden birlikte yaşayan bulutlardaki yan kanal saldırılarına genel bir çözüm olarak VM göçünü önererek kaynak verimli, ölçeklenebilir, gerçek zamanlı hareketli hedef savunmasını kullanan MIGRATE isimli bir konteyner yönetim çerçevesi geliştirmişlerdir. Önerilen çerçevenin farklı ana bilgisayarlar arasında Linux kapsayıcılarında bulunan bulut kiracı uygulamalarının etkili bir şekilde gerçek zamanlı olasılıksal rastgele göçlerini kullandığı belirtilmektedir. Göç süreci, konteyner içerisinde yapılan işleri kaydetmek için çalışan konteyneri kontrol ederek başlamaktadır. Bu özellik mevcut hipervizörler tarafından varsayılan olarak etkin değildir. Çalışan uygulamaların kontrol noktasını etkinleştirmek için kullanılan kontrol işaretleme aracı, kullanılan dosyaların ve bellek içeriğinin anlık görüntüsünü alarak çalışan konteyner ve içerisindeki uygulamaları anlık olarak dondurmaktadır. Yapılan deneyler sonucunda saldırganın konteyner konumlarını önceden bilmemekle birlikte, göç sayısını artırmanın başarılı yan kanal saldırılarını hafiflettiği görülmüştür.

e. VM kaçışına karşı önlemler (Countermeasures against VM escape)

HyperSafe [37]:

Hipervizörün akış kontrol bütünlüğünü sağlamaya yarayan bir yaklaşımdır. Bu yaklaşımda hedef, yazmaya karşı korumalı bellek sayfalarının değiştirilmesine engel olan geçirilemeyen "bellek kilidi" ve kontrol verilerini işaretçi dizine dönüştüren "kısıtlı keskin indeksleme" olmak üzere iki yöntem ile tip 1 hipervizörlerin korunması amaçlanmıştır.

Güvenilir bulut bilişim platformu [23]:

Güvenilir sanal makine monitörü ve güvenilir bir koordinatörden oluşan TCCP (Trusted Cloud Computing Platform), sağlayıcılara kapalı kutu çalışma çevresi sağlar ve kullanıcılara VM'lerini başlatmadan önce ortamın güvenliğini belirlemeye izin verir.

Güvenilir sanal veri merkezi [24][25]:

Bulut çevresinde bütünlüğü ve izolasyonu garanti altına almaktadır. Ortak amaçlara sahip sanal makineleri güvenilir sanal alanlar adı altında iş yüklerine göre gruplandırmakta ve zorunlu erişim kontrolü, hipervizör tabanlı izolasyon ve VLAN'lar gibi korunmuş iletişim kanallarını zorlayarak iş yükleri arasında izolasyon sağlar. Ayrıca sistemin bütünlüğünü korumak için yükleme zamanı doğrulama mekanizması kullanarak bütünlük sağlamaktadır.

f. Kötücül sanal makine oluşturmaya karşı önlemler (Countermeasures against malicious virtual machine)

Mirage:

Çalışma [26]'da yazarlar bulut bilişim çevresinde bir sanal makine görüntü yönetim sistemi önermişlerdir. Bu yaklaşım; erişim kontrol çerçevesi, görüntü filtreleri, kaynak tarama ve depo bakım hizmeti olmak üzere birçok güvenlik önlemi içermektedir. Fakat bu yaklaşımda filtreler görüntülerden tüm kötücül yazılımları tarayamayabilir veya hassas verileri silebilmektedir.

Clustering:
Bazm ve arkadaşları [83] ağ parametrelerinin analizine dayalı bulut üzerinde kötücül davranışları tespit etmek için bir yaklaşım önermişlerdir. Bu yaklaşım hem Entropi hem de kümeleme yöntemlerini ağ parametreleri üzerine uygulayan kaynak tabanlı bir saldırı tespitidir. Benzer VM'leri otomatik olarak kümeleyerek VM'lerin davranış izlemesini ele almak amaçlanmaktadır. Yaklaşımın amacı aynı kötücül yazılımı çalıştıran VM'leri bir araya getirmek ve bu nedenle ağ parametrelerinin değişimi açısından benzer davranışları göstermektir. Bu fikir arkasındaki motivasyonun aynı veri merkezinde anormal davranışa sahip tüm kötü niyetli VM'leri toplu olarak tespit etme ihtiyacı olduğu belirtilmektedir.

Deshpande ve Ainapure [84] kötücül ya da anormal saldırıların hedefi olan VM'leri saldırıdan korumak için VM'lerin durumunu gösteren VM izleme sistemi önermektedir. Önerilen sistem, hangi VM'in VMM'e saldırdığını veya hangi VM'lerin diğerlerine saldırdığını belirlemek için farklı saldırıları sınıflandırabilen ve bellek dökümlerini analiz eden Nitro VM izleme aracını kullanarak statik ve dinamik VM durumunu izlemektedir.

g. Güvensiz sanal makine göçüne karşı önlemler (Countermeasures against insecure virtual machine migration)

VM'in canlı göçü için korunma önlemleri (PALM):
Çalışma [27]'de göç sırasında ve sonrasında gizliliği koruyan ve bütünlüğü sağlayan güvenli bir canlı göç çerçevesi önerilmiştir. Sistemin prototipi Xen ve Gnu Linux platformları üzerinde uygulanmıştır. Değerlendirme sonucunda bu şemanın yalnızca şifreleme ve deşifreleme nedeniyle hafif kesinti ve geçiş süresi eklediği görülmüştür.

VNSS:
Çalışma [28]'de her sanal makine için güvenlik poliçelerini özelleştiren bir güvenlik çerçevesi önerilmiştir ve bu çerçeve sanal makine canlı göç yoluyla sürekli koruma sağlamaktadır. Kapsamlı güvenlik duvarı teknolojileri ve ip tabloları, xml komutları kullanıcı alanlı araçlar kullanarak Xen hipervizörü tabanlı bir prototip sistem uygulamışlardır. Yapılan deneyler sonucunda güvenlik poliçelerinin canlı göç boyunca etkili olduğu gözlemlenmiştir.

Ahmad ve arkadaşları [85] canlı VM göçü süreci için platform bütünlüğünün doğrulanması, ortadaki adam saldırısına karşı kimlik doğrulama, uygun erişim kontrol poliçelerinin sağlanması, göç sırasında VM'in gizliliğinin ve bütünlüğünün sağlanması, saldırganın trafiği yakalayıp tekrar kimlik doğrulamasından geçmesinin önlenmesi ve son olarak açık anahtar sertifikası kullanılarak kaynak ana bilgisayarın VM göç işlemini inkar edememesi gibi güvenlik gereksinimlerinden bahsetmektedir. VM göçü sırasında VM' in gizliliğinin ve bütünlüğünün sağlanmasına çözüm olarak Zhang ve arkadaşları [86], sanal makinedeki işlemlere güvenlik sağlayan VMM koruma sistemi olarak adlandırılan özelleştirilmiş bir VMM' de güvenli VM göçü önermektedir. Korumalı bellek sayfaları da VMM' de saklanır. Önerilen sistem 1) göç işlemi sırasında korunan işlemleri veya sayfaları şifrelemek, şifre çözmek ve engellemek için kullanılan göç verilerini koruma modülü 2) göç işleminden sonra meta verileri (şifreleme anahtarları, işlem kimlikleri vb.) yönetmek için kullanılan meta veri yönetim modülü ve 3) canlı göç işlemi sırasında güvenlik koruması olmak üzere üç modülden oluşmaktadır.

Bir başka çözüm olarak kimlik doğrulama, onaylama ve veri aktarma aşamalarından oluşan Güvenli VM-vTPM (virtual Trusted Platform Module) isimli bir göç protokolü önerilmektedir [87]. İlk aşamada, her iki taraf birbirlerini karşılıklı olarak doğrulayarak sonraki iletişim için güvenli oturum kurmaktadır. Kimlik doğrulama ve güvenli kanal kurulumundan sonra, sistemin bütünlüğünü kontrol etmek / doğrulamak için kaynak tarafından uzaktan onaylama gerçekleştirilmektedir. Son adımda ise VM ve vTPM aktarımı gerçekleşmektedir. Kaynak ana bilgisayar önce VM' i vTPM boyunca askıya alıp şifrelemekte ve sonra hedef makineye aktarmaktadır. Ayrıca, kaynak ana makine vTPM'si boyunca VM'yi de silmektedir.

h. Sanal ağ kandırmaya karşı önlemler (Countermeasures against virtual network spoofing)

Sanal ağ güvenliği: Wu ve arkadaşları [29] sanal makineler arasındaki iletişimi güvenli hale getiren bir sanal ağ çerçevesi sunmuşlardır. Bu çerçeve, köprülü ve yönlendirilmiş olmak üzere

sanal makineler için iki konfigürasyon modu sunan Xen'e dayalıdır. Çerçeve VM'leri dinleme ve kandırma tehlikesinden koruyabilen yönlendirme katmanları, güvenlik duvarı ve paylaşımlı ağlar olmak üzere üç katmandan oluşmaktadır.

Güvenilir sanal alanlar (Trusted Virtual Domains): Cabuk ve arkadaşları [88] erişim kontrolü ve ağ yalıtımı sağlamak için Güvenilir Sanal Alanları (Trusted Virtual Domains-TVD'ler) önermektedir. Erişim kontrolünü desteklemek için gerekli kimlik doğrulama, dijital sertifikalar aracılığıyla sağlanmaktadır. Bu sertifikalar ağa katılan varlıkların kimliğini sağlamakta, ayrıca sistem ağ iletişimindeki varlıkların kimliğini doğrulamak için Sanal Özel Ağları (VPN'ler) kullanmaktadır.

i. Kimlik avına karşı önlemler (Countermeasures against phishing)

Güvenilir Kimlik Bilgileri Yönetimi [4]:

Erişim denetiminde güçlü bir kimlik doğrulama önemli bir güvenlik ihtiyacıdır. Burada kimliği doğrulanmış kullanıcılara yetkiler verilmektedir. Bunun önemli bir yönü kimlik belgelerinin yönetimidir. Federe kimlik yönetimi, bulut tabanlı işbirliği sistemleri gibi açık sistemler için etkili bir çözüm olarak görülmektedir. Güvenilir kimlik yönetimi, güvenilir veri kullanımı yönetimini sağlamak için gereklidir. Sağlanan güvenliğin güvenilirliğini tahmin etmek ve bir bulut hizmet servisi olarak sunulmak üzere yararlı güven değerlendirme metrikleri önerilmektedir. Güvenin değerlendirilmesinin önemi, işbirliğine dayalı güvenli veri paylaşımı, veri analizi ve veri dış kaynak kullanımı için hayati öneme sahiptir.

İki faktörlü doğrulama (Tek seferlik şifre-Biometrik):

Güvenilir kimlik yönetimi için uygulanan bu yöntemde, kullanıcının iki katmanlı kimlik doğrulama yöntemi ile kimliği doğrulanır. İlk olarak kullanıcı, kullanıcı adını ve şifresini girdikten sonra güvenilir bir ikinci iletişim kanalından (e-posta, anlık mesaj servisleri, kısa mesaj servisleri vb.) tek seferlik şifre [59] veya kişinin fiziksel özelliklerine dayanarak bir kişiye özel yüz tanıma, parmak izi gibi bilgiler istenir [15].

Kimlik bilgileri ve güvenli kabuk (shell) anahtarları:

Indu ve arkadaşları [85] kimlik avı saldırılarına karşı dijital güvenlik mekanizmaları olan kimlik bilgileri ve güvenlik kabuk anahtarlarını önermişlerdir. Kimlik bilgileri, otorite, statü, erişim hakları ve hakların kanıtı anlamına gelmektedir. Belirli bir kullanıcının kaynakları ve hizmetleri kullanmayı hak ettiğini göstermektedir. Tek seferlik şifre, kalıp (pattern) ve captcha gibi kimlik bilgilerinin kullanılması, sistemi kötü niyetli faaliyetlerden korumak için geliştirilmiş temel kimlik doğrulama yollarıdır. Bulut ortamında erişim kimlik bilgilerini yönetmek için en sık kullanılan mekanizmalar, Hafif Dizin Erişim Protokolü (LDAP) ve Microsoft Active Directory (AD) teknolojileridir. LDAP ve AD sunucuları, bulut bilişimde kurumsal ağda veya üçüncü taraf satıcılar tarafından yönetilmektedir. Sağlayıcı tarafında kimlik bilgilerini yönetirken, zayıf şifre kurtarma mekanizmaları kullanıldığında zayıf kimlik bilgileri sıfırlama güvenlik açığı gösterilmektedir. Güvenli Kabuk (Secure Shell-SSH) anahtarları, SSH sunucusunu genel anahtar şifrelemesi veya sorun yanıtlama (challenge-response) kimlik doğrulaması yoluyla tanımlamaya yardımcı olmaktadır. SSH anahtarlarının temel avantajı, sunucuya yapılan kimlik doğrulamanın parola ağ üzerinden geçmeden gerçekleştirilmesidir. Bu da parolanın bilgisayar korsanları tarafından ele geçirilmesini veya kırılmasını önlemektedir. Kimlik doğrulama sırasında kaba kuvvet saldırıları yoluyla kimlik bilgilerini tahmin etme girişimleri SSH anahtarları ile azaltılmaktadır. SSH ajanları, her sistem için ayrı şifreler kullanmadan sunucularla bağlantı kurulmasına yardımcı olmaktadır. SSH anahtar temsilcisi, özel anahtarları saklayarak bunları SSH istemci programlarına sunmaktadır. Bu özel anahtarlar parola ile şifrelenmekte ve sunucuya bağlanma girişimleri sırasında parolalar korunmaktadır. Her SSH'ın başlatılmasında, kimlik doğrulama aşamasına geçmeden önce özel anahtarın şifresini çözmek için parolaların kullanılması gerekmektedir. Parola yalnızca ajanın deposuna özel anahtarlar ekleme işlemi sırasında kullanılmaktadır. Bu girişim, sık SSH bağlantıları yapan iletişim cihazlarını desteklemektedir. Oturum başlatıldığında SSH ajanı otomatik olarak çalışmakta ve tüm oturum süresince devam etmektedir.

j. Botnet'lere karşı önlemler (Countermeasures against Botnets)

Wang ve arkadaşları [32] botnet saldırılarını önlemek için işbirlikçi yaklaşım sergileyerek botnet/kötücül bloklama mekanizması, tarama filtreleme ve honeypot uygulanan bir sistem önermişlerdir. Bu mekanizmada buluttan internete giden trafik Snort adı verilen Botnet tespit sunucusuna yansıtılmaktadır. Anti-botnet.tw adresli web sitesinden 5000'den fazla botnet/kötücül yazılım Snort kuralları alınarak anti-botnet kuralı Snort'a uygulanmıştır. Yanlış bir davranış tespit edildiğinde bu yanlış davranış hakkındaki tüm ayrıntılı bilgiyi içeren değişiklikler üretmektedir. Buradaki mekanizma, uyarı bilgisini ayrıştırır ve ilgili bilgileri doğrudan projektör denetleyicisine gönderir. Denetleyici Snort tarafından gönderilen bilgiyi aldıktan sonra kötü amaçlı trafiği izole etmek için anahtara bir OpenFlow kuralı gönderir. Ardından gelen botnet/kötücül davranış içeren trafikler, SDN anahtarında OpenFlow kuralından geçemezler ve ağdan düşürülürler.

Giriş/çıkış filtreleme [86]: En iyi bilinen ve yaygın filtreleme tekniklerinden olan giriş/çıkış filtreleme, korumalı bir ağa girmeye çalışan sahte IP'lerin trafiğini engellemektedir. Temel olarak, giriş filtreleme, yerel bir ağa yönlendirilen kötü niyetli trafiği filtreler ve çıkış filtreleme, yerel bir ağdan çıkan kötü amaçlı trafiği atar. Giriş filtreleme sistemi, önceden tanımlanmış ağın alan öneki ile eşleşen ağa girilmesine olanak tanımaktadır. Bu nedenle, bir saldırgan, önekle eşleşmeyen sahte IP adresi kullanıyorsa, yönlendiricilere atılmaktadır. Böylece, bu filtreleme teknikleri, sahte IP'nin kullanıldığı yerlerde önemli miktarda Botnet saldırısından korunmayı sağlar. Ancak, botnetlerin geçerli IP adreslerinin saldırı sırasında kaynak IP olarak kullanıldığı durumlarda kullanışlı bir mekanizma değildir.

k. Steganografi saldırısına karşı önlemler (Countermeasures against steganography attack)

Thangavel ve arkadaşları [31] tarafından önerilen çerçevede ses, video, görüntü gibi çoklu ortam verilerinin yetkisiz kişilerden korunması için steganografi ve filigran yönteminin birlikte kullanımı gerçekleştirilmiştir. Çevçevede buluta bir görüntü yüklemek isteyen istemci görüntüyü açık anahtar algoritması olan RSA ile şifreleyerek bulutta depolar. Veri gizleme mesajının ve filigranlı içeriğin şifreli görüntüde çakışmasını önlemek için şifrelenmiş görüntü iki parçaya bölünür. İlk yarım görüntü hem LSB (en az önemli bit) hem de RGB yöntemini kullanarak steganografiye (görüntü üzerindeki metinsel verinin saklandığı yer) tabi tutulur. Resmin ikinci yarısı ECC (Eliptik Eğri Kriptosistemi) algoritması kullanılarak filigrana tabi tutulur. Filigran, gizli görüntü verilerini yetkisiz erişime karşı koruyan bir işlem olarak adlandırılmıştır. Buluttan görüntü çekilmek istediğinde kullanıcı tarafından doğrudan deşifreleme yapılmaktadır.

StegAD ((Steganalysis Active Defense):

Liu ve arkadaşları [87] ses steganografi saldırılarına karşı sistemi savunmak için StegAD isimli yeni bir şema önermişlerdir. Bu şema geliştirilmiş RS ve SADI algoritması olmak üzere iki algoritma içermektedir. Geliştirilmiş RS algoritması şüpheli ses steganografi dosyalarını tespit etmek için kullanılmaktadır. SADI ise olası saklanma pozisyonlarını ortaya çıkarmak ve şüpheli dosyaların saklanabileceği yerlerdeki bilgileri engellemek için uygulanmaktadır.

l. VM geri alma saldırısına karşı önlemler (Countermeasures against VM rollback attack)

Szefer ve arkadaşları [89] Hyperwall isimli bir mimari önererek VM geri dönme saldırısını önleme çözümünü, hipervizörün askıya alma/devam etme işlevlerinin devre dışı bırakılmasına dayandırmaktadır. Fakat askıya alma/devam etme özelliği sanallaştırma için önemli bir özellik olduğu ve devre dışı bırakılması daha iyi bir çözüm sağlamadığı ve VM'lerin ön yüklenmesi, askıya alınması ve devam ettirilmesi sırasında son kullanıcıların yer almasının gerektiği belirtilmektedir. Bu durum da sistemin bir VM'i her yeniden başlattığında, göç ettiğinde veya askıya aldığında her seferinde kullanıcıdan izin istemesi anlamına gelmektedir.

Xia ve arkadaşları [36], Hyperwall ile karşılaştırıldığında hipervizörün herhangi bir temel işlevini devre dışı bırakmadan çalışan bir çözüm sunmaktadır. Bu çözümde, yalnızca son kullanıcı, VM aktivitelerinin günlüğünü denetleyerek bir geri alma eyleminin kötü amaçlı olup olmadığını söyleyebilmektedir.

Tablo 4. Saldırılara Yönelik Çözüm Önerileri (Proposed Solution for Attacks)

Saldırı	Çözüm önerileri
Hizmet hırsızlığı	○ Kimlik ve erişim yönetimi rehberliği [30] ○ Dinamik kimlik bilgileri [20] ○ Kullanıcı erişim poliçesi değişimleri [30] ○ Tek kullanımlık şifreler ve belirteç tabanlı kimlik doğrulama [74]
Hizmet aksatma	○ Kaotik Teori [90] ○ Geri izleme, filtreleme, yer paylaşımlı ağ mekanizmaları [75] ○ Atlama (hop) sayısı filtreleme [77] ○ IaaS katmanında güven tabanlı yaklaşım [78] ○ SYN önbellek yaklaşımı, SYN çerezleri savunma yaklaşımı, PaaS katmanında alınan SYN süresinin azaltılması, IaaS katmanında filtreleme ve güvenlik duvarı mekanizması ile birlikte aktif izleme mekanizması [76] ○ PaaS katmanında sanal makinelerin ve IaaS katmanında ağ kaynaklarının yapılandırılması [76] ○ IaaS katmanında dizi sınır kontrol mekanizmasının uygulanması, statik ve dinamik kod mekanizmalarının analizi ve kaynak kod yazımının SaaS katmanında önlenmesi [76]
Müşteri veri manipülasyonu	○ Web uygulama tarayıcıları [5] ○ Dağıtık Erişim Kontrolü [4] [53] ○ Bulutta bir hizmet olarak gizlilik koruma ile veri madenciliği [4] [54] ○ Öznitelik tabanlı şifreleme, vekil yeniden şifreleme [54] ○ Hiyerarşik kimlik tabanlı şifreleme [4]
Veri sızıntısı	○ Bölümleme [21] ○ Sayısal imza [57] ○ Homomorfik şifreleme [4] [56] ○ Vekil yeniden şifreleme [15] ○ Öznitelik tabanlı şifreleme [15]
Kötü amaçlı yazılım enjeksiyonu	○ Dosya Tahsis Etme (FAT) tablosu kullanımı [62] ○ Orijinal servis örneğinin imaj tablosunda şifre (hash) değeri depolama [80]
Çapraz VM yan-kanal	○ OpenStack yazılımı [33] ○ Kriptografik anahtarı birden fazla parçaya bölüp VM'lere dağıtma [81] ○ Hipervizör tabanlı yaklaşımlar [81] ○ MIGRATE (konteyner yönetim çerçevesi) [82]
VM kaçışı	○ HyperSafe [37] ○ Güvenilir Bulut Bilişim Platformu [23] ○ Güvenilir sanal veri merkezi [24] [25]
Kötücül VM oluşturma	○ Mirage (VM görüntü yönetim sistemi) [26] ○ Clustering (kötücül VM'leri bir araya toplayan ve tespit eden sistem) [83] ○ VM izleme sistemi [84]
Güvensiz VM göçü	○ VM'in canlı göçü için korunma önlemleri (PALM) [27] ○ VNSS (her VM için güvenlik poliçelerini özelleştiren bir güvenlik çerçevesi [28] ○ VMM koruma sistemi [86] ○ VM-vTPM (virtual Trusted Platform Module) [87]
Sanal ağların kandırılması	○ Sanal ağ güvenliği [29] ○ Güvenilir sanal ağlar [88]
Kimlik avı	○ Güvenilir kimlik bilgileri yönetimi [4] ○ İki faktörlü doğrulama [59] [15] ○ Kimlik bilgileri ve güvenli kabuk anahtarları [85]
Botnetler	○ Botnet bloklama mekanizması [32] ○ Giriş/çıkış filtreleme [86]
Sesli Steganografi	○ Filigran yöntemi [31] ○ StegAD (Steganalysis Active Defense) [87]
VM geri alma	○ Hyperwall [89] ○ Tüm geri alma eylemlerinin günlüğe kaydedilmesi ve denetlenmesi [88]

Kayıt denetimi ile kullanıcı, şüpheli geri almayı kontrol edebilir ve bulut operatöründen bu tür işlemlerin gerekliliğini kanıtlamasını isteyebilir veya bir VM üzerindeki işlemleri önceden bir geri alma politikası ile kısıtlar veya ikisini birden yapabilir. Her ne kadar bu çözüm, Hyperwall ile karşılaştırıldığında kullanıcı katılımını en aza indirmiş olsa da değişen bulut bilişim altyapısı, VM işletiminin bazı kullanıcı müdahaleleriyle özerk çalışma gerektirmektedir.

Krishna ve Rani [88], tüm geri alma eylemlerinin güvenli bir şekilde günlüğe kaydedilerek ve denetlenerek geri alma saldırısının önlenebileceğini savunmaktadır. Günlük bütünlüğünün korunmasında TPM de kullanılabileceği, ayrıca VM önyüklemesi, VM askıya alma, VM özgeçmiş ve günlüğe kaydetme bilgilerinde kullanılan dört unsur olarak belirtilmektedir. VM'nin bellek sorumlusu olarak izole edilmesi ve şifrelenmesi, belleği korumada yardımcı olmakta, bu nedenle geri alma saldırısı için çözüm oluşturmaktadır. Bu çözüm ayrıca hipervizörün bellek sayfalarını değiştirmesini veya okumasını da önlemektedir. Bulut bilişimin her bir katmanında meydana gelen saldırıları önlemek amacıyla literatürde yer alan çözüm önerileri Tablo 4'te özetlenmiştir.

V. SONUÇ VE ÖNERİLER (CONCLUSION AND RECOMMENDATIONS)

Günümüzde bulut bilişim, ağa bağlı kullanıcılar için hizmetleri barındıracak bir sunucu sağlayarak paylaşılan kaynakların etkili kullanımını hızlı, esnek ve düşük maliyetli bir şekilde sağlamaktadır. Bulut bilişimin bu avantajlarına rağmen bulutta meydana gelen veri ihlali ve denetim eksikliği yüzünden çok büyük şirketler çoğunlukla daha az hassas olan verilerini bulutta saklamaktadırlar. Bulut kullanıcılarının yanı sıra bulut sağlayıcıları için de etkin bir sistem olmasına rağmen çeşitli güvenlik problemleri nedeni ile bulut bilişimin yaygınlaşması engellenmektedir. Bu çalışmada bulut bilişimin faydaları ile birlikte Bulut Güvenlik Birliği (CSA) tarafından yayınlanan güvenlik uyarılarından yola çıkılarak bu uyarılar eşliğinde bulut sağlayıcıların ve kullanıcıların uygulaması gereken önlemlerden bahsedilmiştir. Ayrıca bulut bilişim mimarisindeki katmanlı yapıdan kaynaklanan güvenlik problemleri ele alınarak her katmanın güvenlik zafiyetleri hakkında bilgi verilmiş ve bu zafiyetler kullanılarak saldırganlar tarafından yapılan popüler saldırılar ve tehditler açıklanmıştır. Yapılan araştırmalar sonucunda hizmet hırsızlığı, hizmet aksatma, veri sızıntısı, sesli steganografi, sanal ağların kandırılması, kimlik avı, güvensiz VM göçü gibi toplamda 17 adet bulut güvenlik problemi tespit edilmiştir. Bu tehditler bulut bilişimin her bir katmanında kategorilere ayrılarak açıklanmıştır. Aynı zamanda her bir saldırı için literatürde önerilen çözümler sunulmuştur.

Yapılan araştırmalar doğrultusunda, önerilen çözümler arasında VM atlama, veri temizleme ve hedeflenmiş paylaşılan hafıza saldırılarına özgü bir yaklaşım geliştirilmediği tespit edilmiştir. Fakat bu saldırılara sebebiyet veren zafiyetlerin engellenmesi için üretilen çözümler dolaylı olarak saldırıya da çözüm olabilir. Örneğin hedeflenmiş paylaşılan hafıza saldırısında buluta enjekte edilen kötücül kod aracılığıyla sanal makinelerdeki bellek yığınlarına erişim sağlanabilmektedir. Bunu önlemek için öncelikle kötücül kod enjeksiyonunun engellenmesi gerekmektedir. Çalışma kapsamında kötü amaçlı yazılım enjeksiyonu saldırısı ayrı bir kategoride değerlendirilmiştir. Bu yüzden dolaylı olarak kötü amaçlı yazılım enjeksiyonunun engellenmesi, hedeflenmiş paylaşılan hafıza saldırısına da çözüm olabilir. Benzer şekilde veri temizleme saldırısının zafiyetleri de veri sızıntısı saldırısının zafiyetleri ile eşleşmektedir. Fakat VM atlama saldırısına yönelik doğrudan ya da dolaylı bir çözüm önerisi yapılan araştırmalar doğrultusunda bulunamamıştır. Bu bağlamda VM atlama saldırısı, bulut bilişim tehditlerine yönelik çalışmalarda gelecekteki araştırma gündemi potansiyeline sahiptir. Yeni uygulamalar, hizmetler ve yenilikler bulut bilişimi vazgeçilmez hale getireceğinden dolayı literatürde önerilen bu çözümlerin bulut bilişimi evrimsel bir dayanak noktası olarak tutmaya yardımcı olacağı düşünülmektedir. Fakat bulut bilişim kavramının ilk ortaya çıkmasından bugüne, yenilikler ile birlikte bulut altyapı güvenliğini çökertmeye yönelik daha fazla kişisel ve devlet destekli saldırıların yapılacağı da öngörülmektedir. Siber saldırganlar daha tecrübeli hale geldiğinden dolayı kamu ve özel sektördeki güvenlik analistlerinin de saldırıları tespit ve önleme yöntemlerinde daha tecrübeli ve zamanla yarışır hale gelecekleri

düşünülmektedir. Yapılan araştırmalar eşliğinde buluttaki güvenlik endişelerini minimum indirmek amacı ile siber güvenlik için temel savunma mekanizmaları olarak bilgi güvenliği ve olay yönetimi (SIEM) ve kötücül yazılım sistemleri gibi araçlara yatırımların artırılması gerektiği üzerinde durulmaktadır. Bulut hizmetleri burada önemli bir rol oynayarak bulutun tüm güvenlik önlemlerini uygulayamayan şirketlere güvenli ve erişilebilir hizmetler sunması planlanmaktadır.

KAYNAKLAR (REFERENCES)

[1] Srinivasamurthy S., Liu D., Vasilakos A., Xiong N., Security and Privacy in Cloud Computing: A Survey," Parallel&Cloud Computing (PCC). London, vol. 2, pp126-149, New York, NY: American V-King Scientific Publishing, 2013. http://opus.ipfw.edu/compsci_facpubs/44

[2] CSA Cloud Security Alliance , Top Threats to Cloud Computing", Prepared by the Cloud Security Alliance, March 2010, Erişim tarihi: 13.12.2018

[3] Mell P. Grance T., The NIST Definition of Cloud Computing, 2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/clouddef-v15.pdf, Erişim tarihi: 13.01.2018

[4] Tari Z., Yi X., U.S. Premarathe, P. Bertok, and I. Khalil, Security and Privacy in Cloud Computing: Vision, Trends, and Challenges, IEEE Cloud Computing published by The IEEE Computer Society, 2015

[5] Morsy M. Grundy J. Müller I., An Analysis of the Cloud Computing Security Problem, In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th November 2010.

[6] Hashizume K.,. Rosado D. G., Fernandez-Medina E., and Fernandez E. B., An Analysis of security issues for cloud computing, Journal of Internet Services and Applications, 4:5, 2013. http://www.jisajournal.com/content/4/1/5

[7] Khan M. A., A Survey of security issues for cloud computing, Journal of Network and Computer Applications, Science Direct Elsevier, pp. 1129, 2016

[8] Khalil I. M., Khreishah A., and Azeem M., Cloud Computing Security: A Survey, Computers, 3, 1-35; doi:10.3390/computers3010001, 2014. www.mdpi.com/journal/computers

[9] CSA Top Threats Working Group, The Notorious Nine- Cloud Security Top Threats, February 2013, Erişim tarihi: 13.12.2018

[10] Cloud Security Alliance, Security guidance for critical areas of focus in Cloud Computing V3.0, 2011. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, Erişim tarihi: 10.01.2018

[11] Ayyub M. Kaushik P., "An Analysis of Security Attacks on Cloud wrt SaaS", Int. Journal of Advancements in Research & Technology, Vol.4, No. 2, February 2015.

[12] Ju J., Wang Y., Fu, J., Wu J., and Lin Z., Research on Key Technology in SaaS, International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington, DC, USA, pp 384–387, 2010

[13] Alimuzzaman A Survey on Cloud Security, Challenges and Mitigation, Scientific Research Journal (SCIRJ), Volume III, Issue VI, pp. 31-36, June 2015

[14] Cloud Security Alliance (CSA), Security guidance for critical areas of Mobile Computing, 2012. Available: https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf, Erişim tarihi: 10.01.2018

[15] Sridhar S., Smys Dr. S., A Survey on Cloud Security Issues and Challenges with Possible Measures, International Conference on Inventive Research in Engineering and Technology, 2016

[16] Chandramouli R. Mell P., State of Security readiness. Crossroads 16 (3):23–25,2010

[17] OWASP (2010) The Ten most critical Web application Security risks. Available: https://www.owasp.org/index.php/Category: OWASP_Top_Ten_Project

[18] Reuben JS., A survey on virtual machine Security. Seminar on Network Security, 2007

[19] Hashizume K., Yoshioka, N., Fernandez EB., Three misuse patterns for Cloud Computing. Rosado DG, Mellado D, Fernandez-Medina E, Piattini M ed) Security engineering for Cloud Computing: approaches and Tools. IGI Global,

Pennsylvania, United States, pp 36–53, 2013

[20] Xiao S., Gong W., "Mobility Can help: protect user identity with dynamic credential", 11th International conference on Mobile data Management (MDM). IEEE Computer Society, Washington, DC, USA, pp 378–380, 2010

[21] Wylie J., Bakkaloglu M., Pandurangan V., Bigrigg M., Oguz S., Tew K., Williams, C., Ganger G. Khosla P., Selecting the right data distribution scheme for a survivable Storage system, CMU-CS-01-120, Pittsburgh, PA, 2001

[22] Harnik D. Pinkas B., Shulman-Peleg A., Side channels in Cloud services: deduplication in Cloud Storage, IEEE Security Privacy 8(6):40–47, 2010

[23] Santos N. Gummadi KP., Rodrigues, R., Towards Trusted Cloud Computing, Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California. USENIX Association Berkeley, CA, USA, 2009

[24] Berge S., Cáceres R., Pendarakis D., Sailer R., Valdez E., Perez R., Schildhauer W., Srinivasan D., TVDc: managing Security in the trusted virtual datacenter, SIGOPS Oper. Syst. Rev. 42(1):40–47, 2008

[25] Berger S., Cáceres R. Goldman K. Pendarakis D. Perez R., Rao JR. Rom E. Sailer R. Schildhauer W., Srinivasan D., Tal S. Valdez E., Security for the Cloud infrastructure: trusted virtual data center implementation, IBM J Res Dev 53 (4):560–571, 2009

[26] Wei J., Zhang X., Ammons G. Bala V. Ning P., Managing Security of virtual machine images in a Cloud environment, Proceedings of the 2009 ACM workshop on Cloud Computing Security. ACM New York, NY, USA, pp. 91–96, 2009

[27] Zhang F., Huang Y., Wang H., Chen H. Zang B., PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection, Trusted Infrastructure Technologies Conference, 2008. APTC'08, Third Asia-Pacific. IEEE Computer Society, Washington, DC, USA, pp 9–18, 2008

[28] Xiaopeng G., Sumei W., Xianqin C., VNSS: a Network Security sandbox for virtual Computing environment, IEEE youth conference on information Computing and telecommunications (YC-ICT). IEEE Computer Society, Washington DC, USA, pp 395–398, 2010

[29] Wu Ding Y., Winer C., Yao L., Network Security for virtual machine in Cloud Computing, 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18–21, 2010

[30] Tirumala S., Sathu H., and Naidu V., Analysis and Prevention of Account Hijacking based INCIDENTS in Cloud Environment, International Conference on Information Technology, pp. 124-129, 2015

[31] Thangavel M., Varalakshmi P. Renganayaki S., Subhapriva G.R., Preethi T., and Banu A. Z., SMCSRC-Secure Multimedia Content Storage and Retrival in Cloud, Fifth International Conference on Recent Trends In Information Technology, 2016

[32] Wang C., Lin C., Liao I., and Kao C., An OpenFlow-based Collaborative Intrusion Prevention System for Cloud Networking, Communication Software and Networks (ICCSN), pp. 85-92, 2015

[33] Kumar B., Abhishek K., Kumar A., Singh M.P., System and Method for Mitigating Cross VM Attacks in Cloud Computing by Securing the Network Traffic, Computer Applications & Industrial Electronics (ISCAIE), pp. 221-225, 2015

[34] Singh S., Pandey B.K., Srivastava R., Rawat N., Rawat P., and Awantika, Cloud Computing Attacks: A Discussion With Solutions, Open Journal of Mobile Computing and Cloud Computing, vol. 1, no. 1, 2014

[35] Nenvani G., and Gupta H., A Survey on Attack Detection on Cloud using Supervised Learning Techniques, Symposium on Colossal Data Analysis and Networking (CDAN), 2016

[36] Xia Y., Liu Y., Chen H., and Zang B., Defending against VM Rollback Attack, Dependable Systems and Networks Workshops (DSN-W), 2012

[37] Wang Z., and Jiang X., HyperSafe: a Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity, Security and Privacy, IEEE Computer

Society, Washington, DC, USA, pp. 380-395, 2010

[38] Freet D. Agrawal R. John S., and Walker J., Cloud Forensics Challenges from a Service Model Standpoint: IaaS, PaaS and SaaS, MEDES '15, October 25-29, pp. 148-155, Caraguatatuba, Brazil, 2015

[39] Li X., Zhou L. Shi Y., and Guo Y., A Trusted Computing Environment Model in Cloud Architecture, Ninth International Conference on Machine Learning and Cybernetics, Qingdao, 11-14, pp. 2843-2848, 2010

[40] Karame G., Neugschwandtner M., Önen M., and Ritzdorf H., Reconciling Security and Functional Requirements in Multi-tenant Clouds, ASIA CCS '17, April 02-06, Abu Dhabi, United Arab Emirates, 2017

[41] Puzio P., Molva R., Önen M., and Loureiro S., PerfectDedup: Secure Data Deduplication, DPM, QASA: Data Privacy Management, and Security Assurance pp 150-166, 2015

[42] Yan Z., Deng R., and Varadharajan V., Cryptography and Data Security in Cloud Computing, Information Sciences 387, pp. 53–55, 2017

[43] Ali M., Khan S., and Vasilakos A., Security in cloud computing: Opportunities and challenges, Information Sciences 305, pp. 357–383, 2015

[44] Krutz R., and Vines D., Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, 2010

[45] Dawoud W., Takouna I., and Meniel C., Infrastructure as a Service Security: Challenges and Solutions, 7th International Conference - Informatics and Systems (INFOS), 2010

[46] Ahmad A., Nasser N., and Anan M., An Identification and Prevention of Theft-of-Service Attack on Cloud Computing, International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT), 2016

[47] Deshmukh R., and Devadkar K., Understanding DDoS Attack & Its Effect In Cloud Environment, Procedia Computer Science, Volume 49, pp. 202-210, 2015

[48] Wang Z., Yang R., Fu X., Du X., and Luo B., A Shared Memory based Cross-VM Side Channel Attacks in IaaS Cloud, 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS): BigSecurity 16: The Fourth International Workshop on Security and Privacy in Big Data, 2016

[49] Hashizume K., Yoshioka N., and Fernandez E., Misuse Patterns for Cloud Computing, AsianPLoP '11 Proceedings of the 2nd Asian Conference on Pattern Languages of Programs, Article no. 12, Tokyo, Japan, 2011

[50] Masti R. J., On the security of Virtual Machine migration and related topics, Master Thesis, Master of Science in Computer Science, ETH Zurich, April 2010

[51] Mahalingam M. S., and Nagarajan M.K., Cloud Based Security Center: To Protect Networking Attack by Forensic Scrutiny, International Journal of Scientific Engineering and Technology, Volume no.3, Issue no. 3, pp. 280-284, 2014

[52] Kebande V. R., and Venter H.S., A Cognitive Approach for Botnet Detection Using Artificial Immune System in the Cloud, Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 52-57, 2014

[53] Almutairi A., Sarfraz M., Basalamah S., Aref W., and Ghafoor A., A Distributed Access Control Architecture for Cloud Computing, IEEE Software, Volume: 29, Issue: 2, pp. 36-44, 2012

[54] Shao J., Lu R., and Lin X., Fine-Grained Data Sharing in Cloud Computing for Mobile Devices, IEEE Conference on Computer Communications (INFOCOM), pp. 2677- 2685, 2015

[55] Li J. Wang Q., Wang C., and Ren K., Enhancing Attribute-Based Encryption with Attribute Hierarchy, Journal of Mobile Networks and Applications, Springer-Verlag New York, Inc. Secaucus, NJ, USA, Volume 16, Issue 5, pp. 553-561, 2011

[56] Tebaa M., El Hajji S., and El Ghazi A., Homomorphic encryption method applied to Cloud Computing, Network Security and Systems (JNS2), pp.86-89, 2012

[57] Rewagad P., and Pawar Y., Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing, Communication Systems and Network Technologies (CSNT), pp. 437-439, 2013

[58] Somani U., Lakhani K., and Mundra M., Implementing digital signature with RSA

encryption algorithm to enhance the Data Security of cloud in Cloud Computing, Parallel Distributed and Grid Computing (PDGC), pp. 211-216, 2010

[59] Huang C., Ma S., and Chen K., Using one-time passwords to prevent password phishing attacks, Journal of Network and Computer Applications 34, pp. 1292–1301, 2011

[60] Grobauer B., Walloschek T., and Stocker E., Understanding Cloud Computing Vulnerabilities, IEEE Security & Privacy, Volume: 9, Issue: 2, pp. 50-57, 2011

[61] Wang K., and Hou Y., Detection Method of SQL injection Attack in Cloud Computing Environment, Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), pp. 487-493, 2016

[62] Zunnurhain K., and Vrbsky S., Security Attacks and Solutions in Clouds, 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, 2010

[63] Aviram A., Hu S., Ford B., and Gummadi R., Determinating timing channels in compute clouds, ACM Workshop on Cloud Computing Security Workshop (CCSW '10); ACM: New York, NY, USA, pp. 103–108, 2010

[64] Hlavacs H., Treutner T., Gelas J., and Lefevre L. Orgerie A., Energy consumption side-channel attack at virtual machines in a cloud, IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), Sydney, NSW, Australia, pp. 605–612, 2011

[65] Jasti A., Shah P., Nagaraj R., and Pendse R., Security in multi-tenancy cloud, IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35–41, 2010

[66] Wu H., Ding Y., Winer C., and Yao L., Network Security for virtual machine in Cloud Computing, 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18–21, 2010

[67] Rocha F., and Correia M., Lucy in the sky without diamonds: Stealing confidential data in the cloud, IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSNW '11), Hong Kong, IEEE Computer Society: Washington, DC, USA, 2011; pp. 129–134, 2011

[68] Tupakula U., Varadharajan V., and Akku N., Intrusion detection techniques for infrastructure as a service cloud, IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), Sydney, Australia, pp. 744–751, 2011

[69] Aborujilah A., and Musa S., Cloud-Based DDoS HTTP Attack Detection Using Covariance Matrix Approach, Hindawi Journal of Computer Networks and Communications, Volume 2017, 2017

[70] VivinSandar S., and Shenai S., Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks, International Journal of Computer Applications, Volume 41, No. 20, 2012

[71] Fan L., Wenhua Z., Yi J., Jianmin L., and Qi L., A Group Tracing and Filtering Tree for REST DDos in Cloud Computing, International Journal of Digital Content Technology and its Applications, vol 4, Number 9, Dec. 2010

[72] Wang L. and Laszewski G., Scientific Cloud Computing: Early Definition and Experience, CiteSeerX, October 2008

[73] Zissis D. and Lekkas D., Addressing cloud computing security issues, Future Generation Computer Systems 28, pp. 583–592, 2012

[74] Khan A. A., Preventing Phishing Attacks using One Time Password and User Machine Identification, International Journal of Computer Applications, Vol. 68, No:3, April 2013

[75] Gupta M., Gopalakrishnan G., and Sharman R., Countermeasures against Distributed Denial of Service, 11th Annual Symposium on Information Assurance (ASIA'16), June 8-9, pp. 6-12, 2016

[76] Darwish D., Ouda A., and Capretz L. F., Cloud-based DDoS Attacks and Defenses, Information Society (i-Society), 2013 International Conference, pp. 67-71 2013

[77] Wang H., Jin C., and Shin K. G., Defense Against Spoofed IP Traffic Using Hop-Count Filtering, IEEE/ACM Transactions on Networking, vol. 15, no. 1, pp. 40–53, Feb. 2007.

[78] J. M. Gonzalez, M. Anwar, and J. B. D. Joshi, A trust-based approach against IP-spoofing attacks, 2011 Ninth Annual International Conference on Privacy, Security and Trust, pp. 63–70, Jul. 2011.

[79] Internet adresi: https://cloud-techlife.com/2017/08/12/major-attacks-on-cloud-computing-with-countermeasures/, Erişim tarihi: 05.05.2019

[80] Shaikh A., Attacks on Cloud Computing and its Countermeasures, International conference on Signal Processing, Communication, Power and Embedded System (SCOPES), pp.748-752, Paralakhemundi - India, 2016

[81] Yang C., Guo Y., Hu H., Liu W., and Wang Y., An effective and scalable VM migration strategy to mitigate cross-VM side channel attacks in cloud, China Communications, Vol. 16, Issue 4, pp.151-171, 2019

[82] Azab M., and Eltoweissy M., MIGRATE: Towards a Lightweight Moving-target Defense against Cloud Side-Channels, IEEE Security and Privacy Workshops, pp. 96-103, 2016

[83] Bazm M., Khatoun R., Begriche Y., Khoukhi L., and Chen X., and Serhrouchni A., Malicious virtual machines detection through a clustering approach, International Conference on Cloud Technologies and Applications (CloudTech), Morocco, 2015

[84] Deshpande S., and Ainapure B., An Intelligent Virtual Machine Monitoring System Using KVM for Reliable and Secure Environment in Cloud, IEEE International Conference on Advances in Electronics, Communication and Computer Technology, Rajarshi Shahu College of Engineering, Pune India, 2016

[85] Indu I., Anand P. M. R., and Bhaskar V., Identity and access management in cloud environments: Mechanisms and challenges, Engineering Science and Technology, an International Journal 21, pp.574-588, 2018

[86] Mahjabin T., Xiao Y., Sun G., and Jiang W., A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, vol 13 (12), 2017

[87] Liu B., Xu E., Wang J., Wei Z., Xu L., Zhao B., and Su J., Thwarting Audio Steganography Attacks in Cloud Storage Systems, International Conference on Cloud and Service Computing, pp. 259-265, 2011

[88] Krishna S. R., and Rani B. P., Virtualization Security Issues and Mitigations in Cloud Computing, Proceedings of the First International Conference on Computational Intelligence and Informatics, pp. 117-127, 2017

[89] Szefer J., and Lee R.B., Architectural support for hypervisor-secure virtualization, SIGARCH Comput. Arch. News, 40, 437–450, 2012

[90] Iyengar N. Ch. S. N., and Ganapathy G., Chaotic Theory based Defensive Mechanism against Distributed Denial of Service Attack in Cloud Computing Environment, International Journal of Security and Its Applications, Vol.9, No.9, pp. 197-202, 2015.