Bulut Bilişim Güvenliğindeki Zorluklar ve Güncel Çalışmalar Üzerine Bir İnceleme

Literatür Makalesi/Review Article

Sercan GÜLBURUN, Murat DENER

Bilgi Güvenliği Mühendisliği Bölümü, Fen Bilimleri Enstitüsü, Gazi Üniversitesi, Ankara Türkiye
sercan.gulburun@gazi.edu.tr, muratdener@universite.edu.tr
(Geliş/Received:25.06.2021; Kabul/Accepted:25.11.2021)
DOI: 10.17671/gazibtd.957461

Özet— Bulut bilişim sistemleri, kişi ve organizasyonlar tarafından ihtiyaç duyulan farklı seviye ve nitelikteki bilgi sistemleri kaynaklarının, talebe bağlı olarak istenilen zaman ve miktarda ihtiyaç sahibine sunulabildiği, çoğunlukla internet üzerinden erişilebilir kılınan, özellikle değişken iş yüklerine sahip organizasyonların ihtiyaçlarına en iyi şekilde cevap verebilen sistemlerdir. Bulut bilişim sistemlerinin kullanımının artmasına paralel olarak hem bulut bilişim platformlarına hem de bu platformlardan servis alan organizasyonlara yönelik saldırılar artış göstermiştir. Çalışmada, öncelikle, farklı kuruluşlar tarafından hazırlanan bulut bilişim güvenlik raporları incelenerek, bulut bilişim kapsamında karşılaşılan temel tehditler ortaya konmuştur. Daha sonra Web of Science veri tabanı temel alınarak bulut bilişim güvenliği kapsamında yapılan güncel çalışmalar incelenmiştir. Güncel çalışmalar Uygulama Güvenliği, Denetim Güvenliği ve Veri Bütünlüğü, Kimlik Yönetimi ve Doğrulama, Erişim Kontrolü ve Yetkilendirme, Veri Paylaşımı, Dağıtık Hizmet Dışı Bırakma (DDoS), Sızma Tespiti ve Ağ Güvenliği, Çoklu Bulut Güvenliği, Gizlilik, Kaynak ve Altyapı Güvenliği, Depolama Alanı Güvenliği, Sanal Makine Güvenliği başlıkları altında sınıflandırılarak sunulmuştur. Gerçek dünya sorunları ile yapılan akademik çalışmalar birlikte değerlendirilmiş ve hangi güvenlik alanlarında çalışmalara ihtiyaç duyulduğu belirlenmiştir.

Anahtar Kelimeler— bulut bilişim, güvenlik, çoklu bulut, gizlilik

A Review on Challenges in Cloud Computing Security and Recent Researchs

Abstract— Cloud computing systems are systems in which information systems resources of different levels and qualities needed by individuals and organizations are offered to the needy at the desired time and amount depending on the demand. Cloud computing systems are mostly made available over the internet and they can meet the needs of organizations with variable workloads in the best way. In parallel with the increase in the use of cloud computing systems, attacks against both cloud computing platforms and organizations receiving services from these platforms have increased. In this paper, first of all, cloud computing security reports prepared by different organizations were examined and the main threats encountered in cloud computing were revealed. Then, based on the web of science database, recent studies within the scope of cloud computing security were examined. Recent studies are grouped and examined under the following categories: Application Security, Audit Security and Data Integrity, Identity Management and Authentication, Access Control and Authorization, Data Sharing, Distributed Denial of Service (DDoS), Intrusion Detection and Network Security, Multicloud Security, Privacy, Resource and Infrastructure Security, Storage Security and Virtual Machine Security. Finally, academic studies and real-world problems were evaluated together and security areas on which academic researhes should focus on were determined.

Keywords— cloud computing, security, multicloud, privacy

1. GİRİŞ (INTRODUCTION)

Bilgi teknolojilerinin günlük hayatımızdaki yeri son çeyrek asırda önemli derecede artmış ve artmaya da devam etmektedir. Bu artışa paralel olarak, bilişim altyapısı ve bu altyapıyı yönetecek personel ihtiyaçları da artış göstermiştir. Ortaya çıkan bu artış, özellikle değişken iş yüklerine sahip organizasyonların ihtiyaçlarının karşılanmasını maliyetli hale getirmiştir. Bulut bilişim sistemleri, kişi ve organizasyonlar tarafından ihtiyaç duyulan farklı seviye ve nitelikteki bilgi sistemleri kaynaklarının, talebe bağlı olarak istenilen zaman ve miktarda ihtiyaç sahibine sunulabildiği, çoğunlukla internet üzerinden erişilebilir kılınan, özellikle değişken iş yüklerine sahip organizasyonların ihtiyaçlarına en iyi şekilde cevap verebilen sistemlerdir.

2007 yılından itibaren popülerlik kazanan bulut bilişim kavramı [1], günümüzde dünyadaki en yaygın bilişim altyapısı modellerinden birisi haline gelmiştir. Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü tarafından 2011 yılında yapılan tanımlamada[1], bulut bilişim sisteminin temel karakteristikleri olarak "isteğe bağlı kendi kendine hizmet (on-demand self-service)", "geniş ağ erişimi (broad network access)", "ortak kaynak havuzu (resource pooling)", "hızlı esneklik (rapid elasticity)" ve "ölçülebilir hizmet (measured service)" özelliklerinden bahsedilmiştir.

Bulut bilişim sistemleri, kurulum modellerine göre 4 kategoriye ayrılırlar. Bunlar, hizmet alıcısı tek bir organizasyon olan özel bulutlar, belirli organizasyonlar tarafından paylaşılan topluluk bulutları, kaynakları herkese açık olan kamuya açık bulut ve farklı modellerin birlikte kullanıldığı hibrit bulut modelleridir.

Bulut bilişim hizmetleri, hizmet olarak yazılım (SaaS), hizmet olarak platform (PaaS) ve hizmet olarak altyapı (IaaS) olmak üzere üç temel hizmet modeli ile hizmet sağlayıcılar tarafından sunulmaktadır. Bulut bilişim güvenliği "paylaşılan sorumluluk" anlayışına dayanmakta olup, farklı hizmet modelleri için hizmet alan ve hizmet sağlayıcıların sorumlulukları değişiklik göstermektedir.

Bilgi teknolojilerinin günlük hayatımızdaki yerinin artışına bağlı olarak, bilgi varlıklarına yönelik tehditler ve saldırılar artış göstermiştir. Bulut göçün armasıyla birlikte, tehditler bulut bilişim sistemlerine de yönelmiş olup, bilgi teknolojisi varlıklarına yönelik genel tehditler yanında bulut bilişime özel tehdit unsurları da ortaya çıkmıştır. Haziran 2011'de Microsoft Business Productivity Online Suite ürünlerine gerçekleştirilen saldırı neticesinde Exchange Online ve Sharepoint Online gibi hizmetlere erişim belirli bir süre sağlanamamıştır. Bulut tabanlı dosya paylaşım hizmeti sunan Dropbox'a 2012 yılında gerçekleştirilen saldırı neticesinde ise 68 milyon kullanıcının eposta ve şifre bilgilerini de içeren veriler sızdırılmıştır. Apple firması tarafından kişisel depolama alanı hizmeti sunan ICloud'a 2014 yılında gerçekleştirilen saldırı neticesinde aralarında birçok tanınmış kişinin de bulunduğu kullanıcılara ait kişisel veriler saldırganlar tarafından ele geçirilmiştir. Nisan 2016'da Meksika Ulusal Seçim Enstitüsü'ne gerçekleştirilen saldırı neticesinde 87 milyon Meksika vatandaşının oy bilgisi sızdırılmış, saldırı ile ilgili yapılan araştırmada ise verilerin yerel kanunlara aykırı bir şekilde Amazon Web Hizmetleri (AWS) üzerinde bulunan bir veri tabanında tutulduğu görülmüştür. En büyük bulut hizmet sağlayıcılarından Microsoft'un bulut operasyonlarına ise günde yaklaşık 1.5 milyon saldırı girişimi gerçekleşmektedir[2].

Bulut bilişim, birlikte getirdiği güvenlik tehditlerinin yanında, sunduğu farklı seviye ve kapsamda hizmetlerle organizasyonların siber dayanıklılığının artmasına yardımcı olmaktadır. Bulut ortamında herhangi bir veri tutmak istemeyen organizasyonların dahi kullanabildiği DDoS korunması gibi hizmetler olduğu gibi bütüncül güvenlik yaklaşımıyla organizasyonların güvenlik ihtiyaçlarının hemen hemen hepsini kapsayan hizmetler de mevcuttur.

Yapılan çalışmanın katkıları şu şekildedir:

- Bulut bilişim güvenliği ile ilgili güncel raporlar incelenerek mevcut sorun alanları ve güvenlik ihtiyaçları listelenmiştir
- Son dönemde bulut bilişim güvenliği alanında yapılan çalışmalar incelenerek, araştırma trendleri ortaya konmuştur
- Siber güvenlik ihtiyaçları ve araştırma trendleri değerlendirilerek, araştırmaların yönelmesi gereken alanlar belirtilmiştir

Çalışmanı ikinci bölümünde farklı kuruluşların bulut bilişim güvenlik raporları incelenmiş, üçüncü bölümünde son dönemde yapılan akademik çalışmalara değinilmiş, dördüncü bölümde bulut bilişimin mevcut güvenlik sorunları ile yapılan akademik çalışmaların değerlendirilmesi yapılmıştır.

2. BULUT GÜVENLİK RAPORLARI (CLOUD SECURITY REPORTS)

Bulut bilişim teknolojisi, konum ve sektörden bağımsız biçimde, dünyanın her yerinde şirketleri yeniden şekillendirmiştir [2]. Birçok organizasyon, bilişim hizmetlerini halka açık bulut servis sağlayıcılarının hizmetlerinden faydalanarak sunmaya başlamıştır. Bu değişim ile güvenlik kaygıları ve sorunları da değişiklik göstermiştir.

[1] The State of Cloud Security Report 2020, Sophos, https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx

[2] Allison Linn, Securing the Cloud, Microsoft Story Labs, https://news.microsoft.com/stories/cloud-security/

Cybersecurity Insiders tarafından farklı sektör, seviye ve rollerdeki 653 siber güvenlik uzmanı ile görüşülerek oluşturulan 2020 Bulut Güvenlik Raporunda[3]:

- Organizasyonların %75'inin bulut bilişim güvenliği konusunda oldukça endişeli olduğu,
- Bulut bilişim güvenliği kaygılarının başında %69 ile veri kaybı/sızıntısı ve %66 ile veri gizliliği geldiği, bunları %44 ile olay müdahale ve kimlik bilgilerinin kazara ifşası olduğu,
- En büyük güvenlik tehditlerini %68 ile hatalı konfigürasyon, %58 ile yetkisiz erişim ve %52 ile güvensiz ara yüzler ve API'ların oluşturduğu,
- Katılımcıları %82'sinin geleneksel güvenlik çözümlerinin bulut ortamında tam kabiliyetle çalışmadığını belirttiği,
- Bulut tabanlı güvenlik çözümlerinin kullanılmamasındaki önemli etkenlerden birinin %37 ile veri gizliliği olduğu,
- Katılımcıları %52'inin bulut ortamında güvenlik ihlallerinin geleneksel BT ortamlarına göre daha fazla olacağı düşündüğü, aksini düşünenlerin oranının %17 olduğu,
- Bulut güvenliği kapsamında organizasyonların %69'unun erişim kontrolü, %53'ünün anti-virüs ve gelişmiş tehdit koruması, %49'unun MFA, %46'sının veri şifreleme ve yedekleme çözümlerini kullandığı,
- Katılımcıların %90'ının buluta göç sürecinde uyumluluk kriterlerinin korunmasının çok önemli olduğunu belirttiği,
- %68'inin iki ya da daha fazla sayıda bulut servis sağlayıcısından hizmet aldığı görülmektedir.

Sophos tarafından farklı sektör ve ülkelerden 3521 bilgi teknolojileri yöneticisi ile görüşülerek oluşturulan Bulut Güvenliği Durumu 2020 raporunda[4]:

- Organizasyonların %70'inin bir son bir yılda bir bulut güvenliği ihlali ile karşılaştığı ve %96'sının mevcut bulut güvenlik seviyeleri konusunda endişeli olduğu,
- Organizasyonların %34'ünün zararlı yazılıma, %29'unun veri sızıntısına, %28'inin fidye yazılıma ve %25'inin ise hesap ele geçirmeye maruz kaldığı,
- Türkiye'deki organizasyonların %63 ile dünyada en çok zararlı yazılıma maruz kalan organizasyonlar olduğu,
- Organizasyonların %66'sında ihlallerin hatalı yapılandırma nedeni ile gerçekleştiği, hatalı yapılandırmaların %44'ünün WAF'larda %22'sinin ise diğer bulut kaynaklarında bulunduğu
- Organizasyonların %91'inde Kimlik ve Erişim Yönetim rollerine gereğinden fayda ayrıcalık verildiği, bunun bir risk oluşturduğu
- Güvenlik kaygılarını %44 ile veri kaybı/sızıntısı, %41 ile güvenlik ihlallerinin tanımlanması ve müdahale, %28'ini ise birden çok bulut hizmet sağlayıcısının yönetimi olduğu,
- Veri güvenliği kapsamında, organizasyonların %85'inin veri tabanlarında %65'inin ise depolama hizmetlerinde şifreleme kullanmadığı,
- Fidye yazılımlara maruz kalan verilerin %59'unun halka açık bulutta bulunan veriler olduğu,
- Çoklu bulut kullanan organizasyonların tek hizmet sağlayıcıdan hizmet alan organizasyonlara göre daha fazla saldırıya maruz kaldıkları görülmektedir.

3. GÜNCEL ARAŞTIRMALAR (RECENT RESEARCHES)

Bulut bilişim güvenliği ile ilgili SCI-E veri tabanında bulunan ve güncel çalışmalar taranmış olup, IoT, sınır bilişim ve sis bilişim gibi alanlar temel alınarak yapılan çalışmalar ile odak noktası bulut bilişim güvenliği olmayan çalışmalar çıkarılarak geriye kalan çalışmalar incelenmiştir. Her ne kadar kesin bir sınıflandırma yapmak mümkün olmasa da incelenen çalışmalar araştırma alanlarına göre gruplara ayrılmış olup aşağıda sunulmuştur.

3.1. Uygulama Güvenliği (Application Security)

Literatürdeki çalışmaların çoğu belirli bir saldırı tipine yönelik yapılmış olup, web hizmetlerinin saldırı toleransları açıkça ortaya konmamıştır. Çalışmada [3] çeşitlendirme ve yansıtma tekniklerine dayalı, risk analizi de içeren bir saldırı tolerans çerçevesi sunulmuştur. Uygulama güvenliği kapsamında yapılan bir diğer çalışmada [4] ise uygulama tasarımı aşamasında kullanılmak üzere, bulut güvenlik metriklerini de içerecek şekilde çalışabilen bir risk değerlendirme çerçevesi sunulmuştur.

3.2. Denetim ve Veri Bütünlüğü (Auditing and Integrity)

Bulut bilişimde veri sahipliği ve veri yönetiminin ayrılmış olması, veri sahibinin verinin bulunduğu fiziksel ortamı kontrol edememesi, kullanıcılar tarafından veri bütünlüğünün geleneksel yöntemlerle kontrolünü zorlaştırmıştır. Bulut hizmet sağlayıcıları tarafından yönetilen verinin bütünlüğünün sağlanması kapsamında yapılan çalışmada [5], alandaki diğer şemalardan farklı olarak, blok zincir teknolojisi kullanan öz sertifikalı açık anahtar sistemine sahip bir denetim protokolü sunulmuştur. Tian ve Jing [6] tarafından yapılan çalışmadaki kimlik doğrulama etiketlerinin zafiyetleri sebebiyle, sunulan protokolü geliştirmek amacıyla gerçekleştirilen çalışmada [7] TPM'in açık anahtar üretme ve veri bütünlüğü sağlama çerçevesinin optimize edildiği geliştirilmiş bir bulut depolama alanı denetim protokolü ortaya konmuştur. Üçüncü parti tabanlı bir denetim şemasının sunulduğu çalışmada [8] kullanılan algoritmalar ile homomorfik mesaj doğrulama kodu kullanılan yöntemler kadar başarılı ve aynı zamanda çok daha az hesaplama ve iletişim ek

[3] 2020 Cloud Security Report [ISC2], Cybersecurity Insiders, https://www.cybersecurity-insiders.com/portfolio/2020-cloud-secuity-report-isc2/

[4] The State of Cloud Security Report 2020, Sophos, https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx

yükü getiren bir yöntem ortaya konmuştur. Veri yükleyicinin denetimci karşısında anonim kalması gerektiği yaklaşımını temel alan, sertifika yönetimi ve yüksek hesaplama maliyetleri gibi problemleri ortadan kaldırmayı amaçlayan çalışmada [9], veri bütünlüğünü etkili bir şekilde kontrol eden kimlik tabanlı Kanıtlanabilir Veri Sahipliği (PDP) protokolü sunulmuştur.

3.3. Kimlik Yönetimi ve Doğrulama (Identity Management and Authentication)

Organizasyonlar tarafından bulut hizmetlerini kullanımının artmasına paralel olarak bulut hizmetleri için ihtiyaç duyulan kullanıcı hesaplarının güvenliği de büyük önem kazanmıştır. Veri gizliliği için optimize edilmiş Blowfish algoritması kullanılan çalışmada [10], çok kademeli bir kimlik doğrulama mekanizması ile zararlı oturum açma süreçleri engellenmeye çalışılmıştır. Rangwani ve Om [11] ise iletişim ve hesaplama yüklerinin azaltıldığı güvenli bir kimlik doğrulama protokolü sunmak için hafif kriptografik özet fonksiyonu kullanılmış ve karşılıklı kimlik doğrulama yaklaşımı izlenmiştir.

3.4. Erişim Kontrolü ve Yetkilendirme (Access Control and Authorization)

Bilgi teknolojisi varlıklarının güvenliği kapsamında erişim kontrolü ve yetkilendirme kavramları yerel veri merkezlerinde olduğu gibi bulutta da büyük önem arz etmektedir. Çalışmada [12] blok zincir teknolojisinin özelliklerinden faydalanan, çok otoriteli, özellik tabanlı ve merkezi olmayan bir erişim kontrol sistemi modeli olan BMAC sunulmuştur. Çok otoriteli ve özellik tabanlı bir şema sunan diğer bir çalışmada [13], bulut depolama alanlarında detaylı şekilde yetkilendirme yapılması mümkün kılınmaktadır. Çin'in resmi kriptografi standartlarından biri olan SM9-IBE kullanılarak özellik tabanlı şifreleme şeması sunulan çalışmada [14], eğitim ağacı yapısıyla Dispacthing and Cloud Control platformunda detaylı bir şekilde yetkilendirme yapılabilmesi sağlanmıştır. Bulut servis sağlayıcılarının güvenilmez olduğu varsayımıyla hareket edilen çalışmada [15], çoklu özellik otoritesi ve tek sertifika otoritesinin olduğu çok otoriteli özellik tabanlı şifrelemeli bir erişim kontrol sistemi ortaya koyulmuştur. Özellik tabanlı şifreleme şeması kullanılan diğer bir çalışmada [16], detaylı politikalarla özellik uzayını birleştirilmesi, kullanıcı kontrolü altında ileri ve geri gizliliğin entegrasyonu ve kötücül kullanıcıların takip edilmesi sağlanmış, ayrıca şifre çözme işlemlerinin dış kaynaklarca yapılabilmesine imkân tanınmıştır. Özellik tabanlı şifreleme kullanan, dinamik erişim kontrolü yapabilen ve izlenebilir bir sistemin (TABE-DAC) sunulduğu çalışmada [17], gizli anahtarlarını sızdıran kötücül kullanıcıların izlenebilmesi ve erişim yetkilerinin veri sahipleri tarafından dinamik bir şekilde yönetilmesi amaçlanmıştır. Eşitlik testi ile kimlik tabanlı şifreleme (IBEET) ve tarih damgası tabanlı kimlik doğrulama mekanizmasının kullanıldığı çalışmada [18], veri sahibinin verinin geçerliliğini kontrol etmesine imkân veren ve bulut ortamındaki sunucuların ise sadece şifreli metni alması sağlayan bir temel sunulmuştur. Otoriteden bağımsız, esnek ve uyumlu bir erişim kontrol yaklaşımının sunulduğu çalışmada [19], hassas verilerin güvenliğinin artırılması maksadıyla AES ve RSA algoritmalarının birlikte kullanıldığı kafes tabanlı güvenlik tekniği ile hibrit katmanlı bir yaklaşım izlenmiştir.

3.5. Veri Paylaşımı (Data Sharing)

Bulut bilişim güvenliğinin sağlanması için gizlilik gerektiren verilerin depolama, transfer ve işleme sürecinde güvenliğinin sağlanması önem arz etmektedir. Bu maksatla, şifreleme algoritmaları başta olmak üzere çeşitli teknikler kullanılarak çalışmalar gerçekleştirilmektedir. Çalışmada [20], bulut ortamında güvenli ve etkin beri paylaşımı kapsamında, mevcut vekil yeniden şifreleme şemalarındaki uygulanabilirlik ve güvenlik ile ilgili yetersizlikleri gidermek için, kimlik tabanlı durumsal vekil yeniden şifreleme şeması (RIB-CPRE-CE) sunulmuştur. Bulut ortamında güvenli veri paylaşımı için blok zincir tabanlı şifreli metin politikalı özellik tabanlı şifreleme şemasının (BCAS) ortaya konulduğu çalışmada [21], veri sahiplerinin veriyi çözebilecek kullanıcıları belirlemesine imkân sağlayan, kullanıcı işlemlerini süresiz saklayan bire-çok şifreleme yaklaşımıyla verinin bir kez şifrelenmesinin yeterli olduğu bir sistem sunulmuştur. Dinamik veri paylaşımının denetimi için sertifikasız çok kopyalı açık bütünlük denetim şemasının (CLMRPIA) sunulduğu çalışmada [22], paylaşılan veriye ait imzanın oluşturulması için kullanıcıların gizli anahtarları kullanılarak veri bütünlüğünün sağlanmaktadır. Punitha ve Indumathi [23] tarafından gerçekleştirilen çalışmada, sağlık bilgilerinin kullanımının izlenebilmesi, hesap verilebilirlik kapsamındaki verilerin bütünlüğünün sağlanması için Ateşböceği anahtar üretme algoritmasının da kullanıldığı bir çerçeve (CCIAI-FKGA) sunulmuştur. Ogiela ve Snášel [24] tarafından bulut ortamında veri güvenliğinin sağlanması için yapılan çalışmada anlamsal eşik şeması tekniğinin kullanımı ortaya konmuştur. Bulut güvenliğinin artırılması kapsamındaki çalışma alanlarından bir diğeri anahtar güvenliğidir.

3.6. Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service)

En yaygın saldırı türlerinden biri olan hizmet dışı bırakma saldırıları, yerel veri merkezlerinde olduğu kadar bulut ortamında da tehdit oluşturmaktadır. Bulut servis sağlayıcıları tarafından hem bulut platformunda sunulan hizmetler için hem de yerel veri merkezleri için hizmet dışı bırakma saldırılarına karşı savunma hizmeti verilmekte, aynı zamanda bulut platformları da bu tür saldırılara maruz kalmaktadır. Düşük yoğunluklu bir dağıtık hizmet dışı bırakma saldırısı türü olan ve mevcut yöntemlerin tespit ve etkisinin azaltılması açısından yetersiz kaldığı Shrew saldırılarına karşı Agrawal ve Tapaswi [25] tarafından hem saldırının tespitini ve etkisinin azaltılmasını sağlayan hem de saldırı kaynağını konumlandıran yazılım tabanlı ağ destekli bir mekanizma sunulmuştur. DDoS saldırısı ve normal trafik esnasındaki entropi değişimine dayanan düşük ek hesaplama yüküne sahip bir savunma mekanizması sunulan çalışmada [26], yüksek doğrulukla

tespit yapıldığı ve saldırı etkilerinin hafifletildiği ortaya konmuştur. DDoS saldırılarına maruz kalmış veri ve sağlıklı verinin ayırt edilmesi için derin öğrenme teknikleri kullanılan çalışmada [27], sadece saldırıya maruz kalmış verilerin ayıklanmasıyla sağlıklı verilerin bulut depolama alanlarında saklanması amaçlanmıştır. Bulut ortamında sistem yüklerinin, farklı yük dengeleme yaklaşımlarıyla yönetiminin incelendiği çalışmada [28], yoğun yük altında dinamik yük dengelemenin sisteme gelen isteklerin engellenmesi kapsamında daha iyi performans gösterdiği ortaya konmuştur.

3.7. Sızma Tespiti ve Ağ Güvenliği (Intrusion Detection and Network Security)

Bulut ortamında sızma tespitinde geleneksel sızma tespiti yaklaşımlarının yetersiz kaldığının belirtildiği çalışmada [29], saldırı tespiti için etkili bir özellik seçiminin ve toplu öğrenmenin kullanıldığı bir sızma tespit yaklaşımı sunulmuştur. Veri madenciliğinin ve şifreleme tekniklerinin birlikte kullanıldığı bir model sunan He ve He [30], sürdürülebilir bir sistem güvenliği sağlanmasını amaçlamıştır. Haraketli hedef savunması teknikleri olan karıştırma ve fazlalık ile bunların birleşiminin incelendiği çalışmada [31], tekniklerin bulut ortamındaki etkinliği saldırılamazlık metriği başta olmak üzere çeşitli açılardan karşılaştırılmıştır. Azure bulutunda gerçekleştirilen çalışmada [32], çeşitli veri setleri kullanılarak eğitilen bir toplu öğrenme metodunun, bir web servisi olarak sunulması amaçlanmıştır. Bulut uç noktası koordineli ve çok katmanlı bir toplu öğrenme metodu kullanan CAPTCHA mimarisinin sunulduğu çalışmada [33], güvenlik sağlanırken aynı zamanda uç cihazların kaynaklarından faydalanılarak bulut kaynaklarının kullanımı optimize edilmeye çalışılmıştır.

3.8. Çoklu Bulut Güvenliği (Multi-cloud Security)

Sunulan hizmetler, konum, maliyet, esneklik gibi sebeplerden ötürü birçok organizasyon tek bulut hizmet sağlayıcısı yerine birden fazla hizmet sağlayıcıdan hizmet almaktadır. Son dönemde artan çoklu bulut kullanımı, çoklu bulut güvenliği alanında yapılacak çalışmalara ihtiyacı artırmıştır. Canlı Mod Doğruluk İzleme Mekanizmasının (VM-VMP) sunulduğu çalışmada [34], mekanizma tarafından temin edilen veri bütünlüğü sayesinde kullanıcıların güvenilmez çoklu bulut ortamında etkin ve güvenli şekilde veri bulundurulabilmesi sağlanmıştır. Lahmar ve Mezni'nin [35] bulanık biçimsel kavram analizinden (FFCA) ve yaklaşımlı kümelerden faydalanarak ortaya koyduğu güvenliğe duyarlı çoklu bulut servis kompozisyonu yaklaşımıyla güvenilir olmayan bulut servis sağlayıcıları ve servisleri elenerek, hizmet alımının daha güvenilir bir uzaydan yapılması amaçlanmıştır. Çoklu bulut ortamında sürekli denetim ve izleme tekniklerinin uygulandığı ve değerlendirildiği çalışmada [36], etkin bir değişiklik yönetimi ve yapılandırma kontrolü ile tehdit tespiti sağlanmıştır. Güvenlik ve güvenilirlik kısıtlarının temel alındığı çalışmada [37], kullanıcının ihtiyaç duyduğu kaynak performansını, güvenliği ve güvenilirliği karşılayan kullanıcı görevleri ve kaynaklar arasında bir eşleştirme stratejisi önerilmiştir. Fonksiyon gizliliğinin korunduğu yeni bir dağıtık fonksiyonel imza şemasının sunulduğu çalışmada [38], şemadan faydalanılarak, güvenilir olmayan çoklu bulut ortamlarında doğrulanabilir ve güvenli dağıtık bulut hizmeti sunulabileceğini ortaya koymuştur.

3.9. Gizlilik (Privacy)

Bulut üzerinden verilen hizmetlerin artmasıyla beraber bulut ortamında işlenen ve muhafaza edilen kişisel verilerde de büyük bir artış olmuştur. Çeşitli kanun ve düzenlemelerle korunması zorunlu kılınan kişisel verilerin güvenliğinin sağlanması kapsamında hem bulut servis sağlayıcıları hem de araştırmacılar tarafından çalışmalar gerçekleştirilmektedir. Çalışmada [39], bulut ortamında gizliliğin korunduğu ve gizlilik ihlali yapanların izlenebildiği içerik tabanlı görüntü alma şeması sunulmuştur. Hesaplama hizmetinin dış kaynaklarla gerçekleştirildiği biyometrik doğrulama sistemlerinde gizliliğin korunmasını hedefleyen çalışmada [40] sunucu tarafında işlenen verilerin istemci ortamından çıkmadan şifrelenerek korunması yaklaşımı izlenmiş ve homomorfik şifreleme tekniğinden faydalanılmıştır. Bulut servis sağlayıcıları tarafından sunulan veri madenciliği hizmetinde gizliliği korunmak amacıyla gerçekleştirilen çalışmada [41], hem etkin bir güvenlik sunan hemde düşük hesaplama gücü ihtiyacı bulunan, homomorfik şifreleme ve şifreli metin paketleme tekniğinin kullanıldığı gizlilik korumalı sık öğe seti sorgusu (PPFIQ) şeması sunulmuştur.

3.10. Kaynak ve Altyapı Güvenliği (Resource and Infrastructure Security)

Bulut hizmetleri genel olarak "kullandığın kadar öde" modeli ile sunulan ve kullanıma göre ücretlendirilen hizmetlerdir. Saldırganlar, hesaplama kaynakları başta olmak üzere organizasyonların sahip olduğu bulut kaynaklarına bu kaynakları kendi amaçları doğrultusunda kullanarak ya da kaynakların tüketmesine neden olarak organizasyonlara hem maddi hem de maddi olmayan zararlar verebilirler. Aşırı kaynak kullanımına neden olan hileli kaynak tüketimi saldırılarının tespiti için P-tahmini tespit şemasının sunulduğu çalışmada [42], web sunucusu olay kayıtlarından yararlanılarak eğitilen bir derin öğrenme modeli kullanılmıştır. Çalışmada [43], bulut güvenliğini ve kaynakların otomatik ölçeklenebilirliğini sağlamak için izolasyon ağaçlarının kullanıldığı optimize edilmiş bir anomali tespiti yaklaşımından ve entropi tabanlı uyarlanabilir Krill sürü optimizasyonundan faydalanmıştır. Çok müşteriye hizmet veren bulut konteyner hizmetlerindeki Linux çekirdeği kaynaklı yaşanabilecek veri sızıntısı ele alındığı çalışmada [44], yaşanabilecek veri sızıntıları ve daha geniş kapsamlı saldırıların önlenmesi maksadıyla iki kademeli bir savunma mekanizması sunulmuştur. Bulut güvenliğinin sağlanması kapsamında donanım tabanlı güvenlik çözümlerinin ele alındığı çalışmada [45] Intel TXT, ARM TrustZone, AMD SEV ve Intel SGX teknolojileri incelenerek güvenlik ve fonksiyonellik gibi ana başlıklar altında karşılaştırılmışlardır.

3.11. Depolama Alanı Güvenliği (Storage Security)

Bulut servis sağlayıcıları tarafından organizasyonlara ihtiyaç duyulduğu anda ve ihtiyaç duyulan miktarda depolama alanı sunulabilmesi bulut depolama alanlarına hem kullanım iştahını hem de kullanımı artırmıştır. Organizasyonlar için kritik önem arz eden verilerin bulut ortamında depolanmasına paralel olarak, bulut depolama hizmetlerinin güvenlik ihtiyaçları da artış göstermiştir. Kırılamaz bir bulut depolama alanı çerçevesi oluşturmak için DNA tabanlı bir şifreleme tekniği kullanılan çalışmada [46], çoklu karar alma modeli ile de verilerin uygun depolama sunucularında tutulması amaçlanmıştır. Skyline hesaplamanın bulut ortamında güvenli bir şekilde uygulanmasını amaçlayan çalışmada [47], güvenli bir depolama yapısı oluşturulması için B+ ağaçları ve simetrik şifrelemeden faydalanılmıştır. Herhangi bir sızıntı olması durumunda dahi depolama alanı ve yetkilendirme güvenliğinin sağlanmasını hedefleyen çalışmada [48], sızıntıya dayanıklı sertifika tabanlı oturum şifreleme (CBS) şeması sunulmuştur. Veri tekilleştirme mimarilerinin büyük bir kısmının global indeksleme ve veri gizliliği konusunda yetersiz olduğunu belirten Rasina Begum ve Chitra [49], uygun bir indekslemeye ve veri gizliliğine sahip bir veri tekilleştirme mimarisi (SEEDDUP) önermiştir. Şifreli metin politikalı özellik tabanlı aranabilir şifreleme (CP-ABSE) bulut ortamlarında veri gizliliği ve detaylı erişim kontrolü sağlanması için yaygın olarak kullanılmakta olup, çalışmada [50], kafes tabanlı şifreleme ile zenginleştirilerek kuantum saldırılarına karşı dayanıklı bir model (CP-ABSEL) sunulmuştur. Çok otoriteli özellik tabanlı şifreleme şemalarının kaynak kısıtı bulunan cihazlar için uygun olmadığı noktasından hareketle, çalışmada [51], kaldırılabilir çok otoriteli özellik tabanlı şifreleme (RMA-ABE) şeması önerilmiştir. Hibrit Pailler-Blowfish algoritmasının kullanıldığı çalışmada [52], hesaplama zamanı ve şifreli metin uzunluğu azaltılarak, çoklu bulut ortamlarının da dahil olduğu bulut senaryolarında etkin bir depolama sağlanması amaçlanmıştır. Çalışmada [53], uygulamalara özel arama gereksinimlerini erişilebilir kılan birkaç farklı veri şifreleme şemasını destekleyen, sorgulama ve analitik hesaplamaları mümkün kılan, NoSQL veri tabanları için kullanıcı tanımlı fonksiyonları destekleyen CryptDICE sistemi sunulmuştur. Toplama tabanlı etiket tekilleştirme sisteminin (ATDS) sunulduğu çalışmada [54], yan kanal saldırılarına karşı dayanıklılık için kullanıcı bağlantılı açık anahtar yerine içerik bağlantılı açık anahtar kullanılmıştır. Çalışmada [55], veri depolama hizmetlerinin dış kaynaklardan alındığı ortamlarda kullanılan mevcut aranabilir şifreleme şemalarındaki tek kelime ile arama yapabilme kısıtını ortadan kaldırarak çoklu kelime aranmasına imkân veren ve çoğu benzer metodun aksine dosya güncellemelerini de destekleyen çoklu anahtar kelime aramalı blok zincir etkin açık anahtar şifreleme (BPKEMS) şemasını sunmuştur.

3.12. Sanal Makine Güvenliği (Virtual Machine Security)

Sanal makinalar yerel veri merkezlerinde oldukça yaygın şekilde kullanılmakta olup, organizasyonlar tarafından ihtiyaç duyulan uygulamaların bulut ortamına kolaylıkla aktarılmasında da büyük kolaylıklar sunmaktadır. Bu sebeple, bulut ortamına hızlı ve düşük maliyetle geçiş yapmak isteyen organizasyonlar, bulut servis sağlayıcılar tarafından verilen sanal makine hizmetini yaygın olarak kullanmaktadır. Bulut ortamında bulunan sanal makinelerin mevcut bir servis sağlayıcıdan başka bir servis sağlayıcıya güvenli bir şekilde taşınmasını amaçlayan çalışmada [56], kullanılan güven jetonu ile sanal makinelerin sadece güvenilir ve/veya düzenlemelerle uyumlu bulut platformlarına taşınabilmesi sağlanır. Çalışmada [57], aynı altyapıyı paylaşan sanal makineler kullanılarak gerçekleştirilen sanal makineler arası saldırıların engellenmesi için, mantıksal analiz ilkeleri kullanılarak çatışan kiracılara ait sanal makinelerin, çatışma düzeylerine göre fiziksel olarak ayrılmasını sağlayan bir sanal makine yerleştirme mimarisi (CBAC4C) sunulmuştur. Geleneksel erişim kontrolü ve şifreleme teknolojilerinin, bulut ortamında, kiracıların gizli verilerinin yayılmasını etkin bir şekilde kontrol edemediği varsayımı üzerine gerçekleştirilen çalışmada [58], kiracı tarafından yönetilen, verinin tüm yaşan döngüsü boyunca korunmasını amaçlayan bir akış kontrol çerçevesi ve politika kuralları tasarlanmıştır.

4. TARTIŞMA (DISCUSSION)

Dünyanın en büyük teknoloji şirketlerinin yatırım yaptığı ve başta bu şirketler olmak üzere çeşitli organizasyonlar ve akademik çevrelerce gelişimi desteklenen bulut bilişimin önümüzdeki yıllarda daha yaygın olarak kullanılacağı açık bir şekilde görülmektedir. Sunulan hizmetlerin ve hizmet alan kullanıcıların çeşitlenmesiyle doğru orantılı bir şekilde bulut hizmetlerine yönelik saldırılar da artmıştır ve artmaya devam edeceği öngörülmektedir. Bu sebeple mevcut ve muhtemelen saldırıların en iyi şekilde anlaşılarak bunlara karşı etkin savunma mekanizmaları geliştirilmesi kritik önem arz etmektedir.

2020 yılına yönelik bulut bilişim güvenlik raporları incelendiğinde, bulut bilişim kapsamındaki temel kaygıların veri kaybı, gizlilik ihlali, güvenlik olaylarına müdahale edilmesi ve çoklu bulut kullanımı güvenliği olduğu görülmektedir. Güncel çalışmalar incelendiğinde gizlilik ihlaline yönelik çalışmalara sıkça rastlandığı görülmektedir. Depolama alanı güvenliği, erişim kontrolü ve yetkilendirme ile kimlik yönetimi ve doğrulama alt başlıklarında incelenen makalelerde sunulan yöntemlerin doğrudan ya da dolaylı olarak veri kaybının engellenmesine yönelik olduğu söylenebilir. Organizasyonların çoklu bulut kullanımı hızlı bir şekilde artmaktadır. Her ne kadar çoklu bulut teknolojileri ile ilgili birtakım çalışmalar yayımlanmış olsa da hem çoklu bulut kullanımının artması hem de organizasyonların bilgi sistem mimarilerinin karmaşıklaşması nedeniyle ağ ve kullanıcı hesap güvenliği başta olmak üzere daha fazla çalışmaya ihtiyaç duyulduğu düşünülmektedir. En büyük kaygı alanlarından biri olan güvenlik olaylarına müdahale alanında, esası olay müdahale olan kapsamlı bir çalışma yapılmamış olsa da olay müdahale süreçlerinde kullanılabilecek, sızma ve veri kaçağı tespiti alanlarında

yapılmış çalışmalar mevcuttur. Bulut bilişim uygulamalarına yönelik hem olay müdahale alt süreçleri hem de olay müdahale yaşam döngüsü kapsamında çalışmalara ihtiyaç duyulduğu değerlendirilmektedir.

Bölüm 2'de ele alınan raporlarda, bulut bilişim güvenliğine karşı en büyük tehditler olarak sırasıyla kripto ve fidye yazılımlar başta olmak üzere zararlı yazılımlar, hatalı yapılandırma ve kimlik bilgilerinin çalışması hususları olduğu görülmektedir. Literatürde makine öğrenmesi ve derin öğrenme teknikleri başta olmak üzere farklı teknolojilerle zararlı yazılım tespitine yönelik çok sayıda çalışma olmasına rağmen, güncel çalışmalar incelendiğinde bulut ortamına özgü zararlı yazılım tespitine yönelik çalışmaya rastlanmamıştır. Zararlı yazılım tespiti kapsamında yapılan mevcut çalışmaların bulut ortamında da çalışabileceği değerlendirilmekle birlikte buluta özgü etkin zararlı yazılım tespit yaklaşımlarının geliştirilmesine ihtiyaç bulunmaktadır. Personel yetersizliği ve dikkatsizlik gibi nedenlerle ortaya çıkan hatalı yapılandırma problemi, bulut bilişim kapsamındaki en önemli güvenlik sorunlarından bir tanesidir. Birçok bulut servis sağlayıcısı hem güvenliğin sağlanması hem de çeşitli düzenlemelere uyumluluğun kontrolü kapsamında kontroller sunsa da hatalı yapılandırma probleminin çözülmediği görülmektedir. Kapsamının netleştirilmesi zor olan bir çalışma alanı olarak değerlendirilmekle birlikte, hatalı yapılandırma tespiti üzerine yapılacak çalışmaların bulut bilişim güvenliğinin sağlanmasında önemli bir katkısı olacağı düşünülmektedir. Kullanıcı hesap bilgilerinin çalınması hem bireysel kullanıcılar için hem de organizasyonlar için büyük bir güvenlik tehdidi oluşturmaktadır. 2020 yılı bulut güvenlik raporlarında en önemli üç güvenlik tehdidinden biri olarak karşımıza çıkan kullanıcı hesap bilgilerinin çalışmasının önlemesine yönelik çok faktörlü doğrulama, şifresiz giriş, biyometrik doğrulama gibi alanlarda çalışma ve geliştirmeler yapılmaktadır. Her ne kadar kullanıcı hesap bilgilerinin çalınmasının önlenmesine yönelik metotlar sunulsa da sadece önleyici tedbirler ile güvenliğin sağlanamayacağı açıktır. Hesap bilgilerinin ele geçirilmesi durumunda dahi saldırganların kötücül niyetlerini gerçekleştirmesini engellenmesine ihtiyaç duyulmaktadır. Bu sebeple, kullanıcı davranışı analizi temelli anomali tespiti başta olmak üzere çeşitli anomali tespit yaklaşımları kullanılarak, özellikle ayrıcalıklı hesapların ele geçirildiğinin en kısa sürede tespit edilmesine ve ele geçirilen hesap üzerinden gerçekleştirilebilecek saldırıların etkilerinin en aza indirilmesine yönelik çalışmalara ihtiyaç duyulmaktadır.

5. SONUÇ (CONCLUSION)

Hali hazırda devasa olan ve her geçen gün daha da büyüyen bulut bilişim, özellik gösteren bazı organizasyonlar dışında, bilişim kaynaklarına duyan kurum, kuruluş ve şirketler için ideal bir ihtiyaç karşılama noktasıdır. Dâhil olan yeni organizasyonlar, gelişen teknoloji, sunulan yeni hizmetler gibi hususlarla birlikte bulut platformlar üzerinden verilen hizmetlere yönelik saldırı vektörleri ve saldırılar da artış göstermektedir.

Çalışmada, öncelikle bulut bilişim güvenlik raporları incelenerek gerçek dünyada duyulan kaygılar ve karşılaşılan tehditler ortaya konmuştur. Daha sonra, güncel çalışmalar kategorilere ayrılarak incelenmiştir. Gerçek dünyada karşılaşılan sorunlar ile literatürde yapılan çalışmalar birlikte ele alınarak hangi alanlarda çalışmalara ihtiyaç duyulduğu ortaya konmuştur.

Özellikle insanların içinde bulunduğu ortamlarda, kusursuz bir güvenlik mimarisi yaratmak mümkün görünmemektedir. Gerçek dünya tehditleri göz önünde bulundurulduğunda, gelecekte yapılacak çalışmalarda insan hatalarının önlenmesine ya da bu hataların sebebiyet vereceği saldırıların etkilerinin minimize edilmesine yönelik çalışmalara ihtiyaç duyulduğu görülmektedir.

KAYNAKLAR (REFERENCES)

[1] V. V. Arutyunov, "Cloud Computing: Its History of Development, Modern State, and Future Considerations", *Sci. Tech. Inf. Process.*, 39(3), 173–178, 2012.

[2] M. Alenezi, "Safeguarding Cloud Computing Infrastructure: A Security Analysis", *Computer Systems Science and Engineering*, 37(2), 159-167, 2021.

[3] G. Ouffoué, F. Zaïdi, A. R. Cavalli, H. N. Nguyen, "A Framework for the Attack Tolerance of Cloud Applications Based on Web Services", *Electron.*, 10(1), 1–29, 2021.

[4] A. Sen, S. Madria, "Application Design Phase Risk Assessment Framework Using Cloud Security Domains", *J. Inf. Secur. Appl.*, 55(102617), 2020.

[5] H. Li, F. Guo, L. Wang, J. Wang, B. Wang, C. Wu, "A Blockchain-Based Public Auditing Protocol with Self-Certified Public Keys for Cloud Data", *Secur. Commun. Networks*, 2021(6623639), 2021.

[6] J. Tian, X. Jing, "A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage," *IEEE Access*, 7, 68071–68082, 2019.

[7] H. Yang, Z. Yi, X. A. Wang, Y. Su, Z. Tu, X. Yang, "Improved Lightweight Cloud Storage Auditing Protocol for Shared Medical Data," *Wirel. Commun. Mob. Comput.*, 2021(8886763), 2021.

[8] B. Shao, Y. Ji, "Efficient TPA-based Auditing Scheme for Secure Cloud Storage", *Cluster Computing*, 2021.

[9] H. Yan, W. Gui, "Efficient Identity-based Public Integrity Auditing of Shared Data in Cloud Storage with User Privacy Preserving", *IEEE Access*, 9, 45822-45831, 2021.

[10] [S. I. Shyla, S. S. Sujatha, "Efficient Secure Data Retrieval on Cloud Using Multi-stage Authentication and Optimized Blowfish Algorithm", *J Ambient Intell Human Comput*, 2021.

[11] D. Rangwani, H. Oin, "A Secure User Authentication Protocol Based on ECC for Cloud Computing Environment", *Arab. J. Sci. Eng.*, 46(4), 3865–3888, 2021.

[12] X. Qin, Y. Huang, Z. Yang, X. Li, "A Blockchain-based Access Control Scheme with Multiple Attribute Authorities for Secure Cloud Data Sharing", *J. Syst. Archit.*, 112(101854), 2021.

[13] J. Gu, J. Shen, B. Wang, "A Robust and Secure Multi-authority Access Control System for Cloud Storage", *Peer-to-Peer Netw. Appl.*, 14, 1488-1499, 2021.

[14] H. Ji, H. Zhang, L. Shao, D. He, M. Luo, "An Efficient Attribute-based Encryption Scheme Based on SM9 Encryption Algorithm for Dispatching and Control Cloud", *Conn. Sci.*, 2021.

[15] D. Ramesh, R. Mishra, M. C. Trivedi, "PCS-ABE (t, n): A Secure Threshold Multi Authority CP-ABE Scheme Based Efficient Access Control Systems for Cloud Environment", *J Ambient Intell Human Comput*, 2021.

[16] K. Sethi, A. Pradhan, P. Bera, "PMTER-ABE: A Practical Multi-authority CP-ABE with Traceability, Revocation and Outsourcing Decryption for Secure Access Control in Cloud Systems", *Cluster Comput*, 2, 2021.

[17] L. Guo, X. Yang, W. C. Yau, "TABE-DAC: Efficient Traceable Attribute-Based Encryption Scheme with Dynamic Access Control Based on Blockchain", *IEEE Access*, 9, 8479–8490, 2021.

[18] X. J. Lin, Q. Wang, L. Sun, H. Qu, "Identity-based Encryption with Equality Test and Datestamp-based Authorization Mechanism", *Theor. Comput. Sci.*, 861, 117–132, 2021.

[19] N. Saravanan, A. Umamakeswari, "Lattice Based Access Control for Protecting User Data in Cloud Environments with Hybrid Security", *Comput. Secur.*, 100(102074), 2021.

[20] S. Yao, R. V. J. Dayot, H. J. Kim, I. H. Ra, "A Novel Revocable and Identity-Based Conditional Proxy Re-encryption Scheme with Ciphertext Evolution for Secure Cloud Data Sharing", *IEEE Access*, 9, 42801–42816, 2021.

[21] Y. Zuo, Z. Kang, J. Xu, Z. Chen, "BCAS: A Blockchain-based Ciphertext-policy Attribute-based Encryption Scheme for Cloud Data Security Sharing", *Int. J. Distrib. Sens. Networks*, 17(3), 2021.

[22] J. R. Gudeme, S. K. Pasupuleti, R. Kandukuri, "Certificateless Multi-replica Public Integrity Auditing Scheme for Dynamic Shared Data in Cloud Storage", *Comput. Secur.*, 103(102176), 2021.

[23] A. A. A. Punitha, G. Indumathi, "Centralized Cloud Information Accountability Integrity with Firefly Key Generation Algorithm (CCIAI-FKGA) for Cloud Environment", *Concurr Comput*, 33(3), 2021.

[24] L. Ogiela, V. Snášel, "Intelligent and Semantic Threshold Schemes for Security in Cloud Computing", *Concurr Comput*, 33(2), 2021.

[25] N. Agrawal, S. Tapaswi, "An SDN-Assisted Defense Mechanism for the Shrew DDoS Attack in a Cloud Computing Environment", *J Netw Syst Manag*, 29(2), 1–28, 2021.

[26] A. Mishra, N. Gupta, B. B. Gupta, "Defense Mechanisms Against DDoS Attack Based on Entropy in SDN-cloud Using POX Controller", *Telecommun Syst*, 77, 47-62, 2021.

[27] A. Agarwal, M. Khari, R. Singh, "Detection of DDOS Attack using Deep Learning Model in Cloud Storage Application", *Wirel Pers Commun*, 2021.

[28] Y. Kırsal, E. Caglar, "Bulut Bilişimde Yük Dengeleme Mekanizmasının Analitik Modellemesi ve Performans Değerlendirmesi", *Bilişim Teknolojileri Dergisi*, 14(3), 279-286, 2021.

[29] S. Krishnaveni, S. Sivamohan, S. S. Sridhar, S. Prabakaran, "Efficient Feature Selection and Classification Through Ensemble Method for Network Intrusion Detection on Cloud Computing", *Cluster Comput.*, 2021.

[30] Q. He, H. He, "A Novel Method to Enhance Sustainable Systems Security in Cloud Computing based on the Combination of Encryption and Data Mining", *Sustain*, 13(1), 1–17, 2021.

[31] H. Alavizadeh, J. B. Hong, D. S. Kim, J. Jang-Jaccard, "Evaluating the Effectiveness of Shuffle and Redundancy MTD Techniques in the Cloud", *Comput. Secur.*, 102(102091), 2021.

[32] S. Rajagopal, P. P. Kundapur, K. S. Hareesha, "Towards Effective Network Intrusion Detection: From Concept to Creation on Azure Cloud", *IEEE Access*, 9, 19723–19742, 2021.

[33] Z. Ouyang, X. Zhai, J. Wu, J. Yang, D. Yue, C. Dou, T. Zhang, "A Cloud Endpoint Coordinating CAPTCHA based on Multi-view Stacking Ensemble", *Comput Secur*, 103(102178), 2021.

[34] M. H. Mohammed, "Bio-inspired Approach and Integrity Check Mechanism for Secure Data Storage in Multi-cloud Environment", *J Ambient Intell Human Comput*, 2021.

[35] F. Lahmar, H. Mezni, "Security-aware Multi-cloud Service Composition by Exploiting Rough Sets and Fuzzy FCA", *Soft Comput*, 25(7), 5173–5197, 2021.

[36] K. A. Torkura, M. I. H. Sukmana, F. Cheng, C. Meinel, "Continuous Auditing and Threat Detection in Multi-cloud Infrastructure", *Comput Secur*, 102(102124), 2021.

[37] Q.-H. Zhu, H. Tang, J.-J. Huang, Y. Hou, "Task Scheduling for Multi-Cloud Computing Subject to Security and Reliability Constraints", *IEEE/CAA J Autom. Sin*, 8(4), 848–865, 2021.

[38] M. Liu, L. Wang, Q. Wu, J. Song, "Distributed Functional Signature with Function Privacy and Its Application", *Secur Commun Networks*, 2021, 1–14, 2021.

[39] Z. Wang, J. Qin, X. Xiang, Y. Tan, "A Privacy-preserving and Traitor Tracking Content-based Image Retrieval Scheme in Cloud Computing", *Multimed Syst*, 27, 403-415, 2021.

[40] M. Taheri, S. Mozaffari, P. Keshavarzi, "Privacy-preserving Biometric Verification with Outsourced Correlation Filter Computation", *Multimed Tools Appl*, 80, 21425-21448, 2021.

[41] W. Wu, M. Xian, U. Parampalli, B. Lu, "Efficient Privacy-preserving Frequent Itemset Query over Semantically Secure Encrypted Cloud Database", *World Wide Web*, 24, 607–629, 2021.

[42] A. Agarwal, A. Prasad, R. Rustogi, S. Mishra, "Detection and Mitigation of Fraudulent Resource Consumption Attacks in Cloud using Deep Learning Approach", *J Inf Secur Appl*, 56(102672), 2021.

[43] A. S. Rahumath, M. Natarajan, A. R. Malangai, "Resource Scalability and Security Using Entropy Based Adaptive Krill Herd Optimization for Auto Scaling in Cloud", *Wirel Pers Commun*, 119, 791-813, 2021.

[44] X. Gao, B. Steenkamer, Z. Gu, M. Kayaalp, D. Pendarakis, H. Wang, "A Study on the Security Implications of Information Leakages in Container Clouds", *IEEE Trans. Dependable Secur Comput*, 18(1), 174–191, 2021.

[45] O. Demigha and R. Larguet, "Hardware-based Solutions for Trusted Cloud Computing", *Comput Secur*, 103(102117), 2021.

[46] A. Majumdar, A. Biswas, A. Majumder, S. K. Sood, K. L. Baishnab, "A novel DNA-inspired Encryption Strategy for Concealing Cloud Storage", *Front Comput Sci*, 15(3), 2021.

[47] J. Zhao, Y. Ma, J. Cui, Y. Peng, K. Li, T. Wang, "SecSky: A Secure Dynamic Skyline Query Scheme with Data Privacy", *IEEE Access*, 9, 5690–5703, 2021.

[48] Y. Zhou, Y. Xu, Z. Qiao, B. Yang, M. Zhang, "Continuous Leakage-resilient Certificate-based Signcryption Scheme and Application in Cloud Computing", *Theor Comput Sci*, 860, 1–22, 2021.

[49] B. R. Begum, P. Chitra, "SEEDDUP: A Three-Tier SEcurE Data DedUPlication Architecture-Based Storage and Retrieval for Cross-Domains Over Cloud", *IETE J Res*, 2021.

[50] U. S. Varri, S. K. Pasupuleti, K. V. Kadambari, "CP-ABSEL: Ciphertext-policy Attribute-based Searchable Encryption from Lattice in Cloud Storage", *Peer-to-Peer Netw Appl*, 14, 1290-1302, 2021.

[51] Y. Ming, B. He, C. Wang, "Efficient Revocable Multi-Authority Attribute-Based Encryption for Cloud Storage", *IEEE Access*, 9, 42593–42603, 2021.

[52] B. Seth, S. Dalal, D.C. Le, V. Jaglan, N. Dahiya, A. Agrawal, M.M. Sharma, D. Prakash, K.D. Verma, "Secure Cloud Data Storage System using Hybrid Paillier Blowfish Algorithm", *Comput Mater Contin*, 67(1), 779–798, 2021.

[53] A. Rafique, D. Van Landuyt, E. Heydari Beni, B. Lagaisse, W. Joosen, "CryptDICE: Distributed Data Protection System for Secure Cloud Data Storage and Computation", *Inf Syst*, 96, 2021.

[54] X. Tang, L. Zhou, B. Hu, H. Wu, "Aggregation-Based Tag Deduplication for Cloud Storage with Resistance against Side Channel Attack", *Secur Commun Networks*, 2021.

[55] Z. Chen, A. Wu, Y. Li, Q. Xing, S. Geng, "Blockchain-Enabled Public Key Encryption with Multi-Keyword Search in Cloud Computing", *Secur Commun Networks*, 2021.

[56] M. Aslam, S. Bouget, S. Raza, "Security and Trust Preserving Inter- and Intra-cloud VM Migrations", *Int. J Netw Manag*, 31(2), 1–19, 2021.

[57] M. T. Dlamini, J. H. P. Eloff, H. S. Venter, M. M. Eloff, "CBAC4C: Conflict-based VM Isolation Control for Cloud Computing", *Int Trans Oper Res*, 25(4), 2021.

[58] Z. Zhang, Z. Yang, X. Du, W. Li, X. Chen, L. Sun, "Tenant-Led Ciphertext Information Flow Control for Cloud Virtual Machines", *IEEE Access*, 9, 15156–15169, 2021.