International Journal of Social and Humanities Sciences Research
JSHSR
Uluslararası Sosyal ve Beşeri Bilimler Araştırma Dergisi
Uluslararası Hakemli Dergi- International Refereed Journal
ISSN: 2459-1149

Received-Makale Geliş Tarihi 02.11.2024 *Research Article /Araştırma Makalesi*
Published-Yayınlanma Tarihi 31.12.2024 10.5281/zenodo.14579855
Volume-Cilt (Issue-Sayı), ss/pp 11(114), 2694-2714

Öğr.Gör. Mustafa Of
https://orcid.org/0000-0002-7924-9073
Kocaeli Üniversitesi, Kocaeli Meslek Yüksekokulu, Kocaeli / TÜRKİYE
ROR Id: https://ror.org/0411seq30

Öğr.Gör. İsmail Kılıçaslan
https://orcid.org/0000-0002-8443-9912
Kocaeli Üniversitesi, Ali Rıza Veziroğlu Meslek Yüksekokulu, Kocaeli / TÜRKİYE
ROR Id: https://ror.org/0411seq30

Bulut Bilişimde Veri Güvenliği: Güncel Sorunlar ve Çözüm Önerileri

Data Security in Cloud Computing: Current Problems and Solution Proposals

ÖZET

Bulut bilişim, sağladığı esneklik, maliyet avantajı ve erişilebilirlik gibi özelliklerle modern bilgi teknolojilerinin temel taşlarından biri haline gelmiştir. Ancak, bu teknolojiye olan talebin artışı, veri güvenliği ve mahremiyet konularında ciddi endişeleri beraberinde getirmektedir. Bu makale, bulut bilişimde veri güvenliği ile ilgili güncel sorunları ele almakta ve bu sorunların üstesinden gelmek için önerilen çözüm yöntemlerini tartışmaktadır. Özellikle veri şifreleme, kimlik doğrulama, yetkilendirme mekanizmaları ve yapay zekâ tabanlı güvenlik araçları gibi stratejiler incelenmiştir. Ayrıca, gelecekte veri güvenliğini artırmaya yönelik yeni yaklaşımlar ve teknolojik eğilimler değerlendirilmiştir. Bu çalışma hem araştırmacılara hem de sektör uzmanlarına bulut bilişimde güvenli veri yönetimi konusunda önemli bir rehber sunmayı hedeflemektedir.
Anahtar Kelimeler: Bulut Bilişim, Veri Güvenliği, Şifreleme, Kimlik Doğrulama, Yapay Zekâ, Blockchain, Siber Güvenlik

ABSTRACT

Cloud computing has become one of the cornerstones of modern information technologies with its features such as flexibility, cost advantage and accessibility. However, the increasing demand for this technology raises serious concerns about data security and privacy. This article discusses current issues related to data security in cloud computing and discusses proposed solutions to overcome these issues. In particular, strategies such as data encryption, authentication, authorization mechanisms and artificial intelligence-based security tools are examined. In addition, new approaches and technological trends to improve data security in the future were evaluated. This study aims to provide an important guide on secure data management in cloud computing for both researchers and industry professionals.
Keywords: Cloud Computing, Data Security, Encryption, Authentication, Artificial Intelligence, Blockchain, Cyber Security

1. GİRİŞ

Dijitalleşmenin hız kazanması ve veri hacmindeki büyük artış, bulut bilişim teknolojilerinin modern iş süreçlerinde ve bireysel kullanıcıların hayatında vazgeçilmez bir konuma gelmesini sağlamıştır. Gartner'a (2023) göre, işletmelerin %85'inden fazlası, iş süreçlerinin en az bir bölümünü bulut tabanlı hizmetlerle yürütmektedir. Bulut bilişim, sağladığı esneklik, maliyet avantajı ve ölçeklenebilirlik özellikleri sayesinde hem bireysel kullanıcılar hem de işletmeler için etkili çözümler sunmaktadır (Armbrust vd., 2010). Ancak, bu yaygın kullanım beraberinde veri güvenliği ve mahremiyetle ilgili kritik sorunları da gündeme getirmiştir (Rittinghouse ve Ransome, 2010).

Veri güvenliği, özellikle bulut bilişim ortamında, kullanıcıların en çok endişe duyduğu konuların başında gelmektedir. Çeşitli çalışmalara göre, veri gizliliği, erişim yetkilendirme zafiyetleri, kimlik doğrulama sorunları ve siber saldırılar, bulut bilişimde karşılaşılan temel güvenlik tehditleri arasında yer almaktadır (Zissis ve Lekkas, 2012; Subashini ve Kavitha, 2011). Örneğin, 2021 yılında gerçekleşen Colonial Pipeline siber saldırısı, yalnızca bir hizmet kesintisine değil, aynı zamanda büyük ekonomik kayıplara ve veri güvenliği açıklarına da yol açmıştır (IBM Security, 2024). Bu saldırı, Amerika Birleşik Devletleri'nin en büyük boru hattı şirketinin akaryakıt transferinin aksamasına neden oldu (Russon, 2021). Bu durum, bulut bilişimde etkili güvenlik politikalarının ve yenilikçi çözümlerin geliştirilmesi gerektiğini ortaya koymaktadır.

Literatürde, bulut bilişim güvenliği ile ilgili birçok yaklaşım tartışılmıştır. Şifreleme teknikleri, kimlik ve erişim yönetimi sistemleri, güvenlik duvarları ve makine öğrenimi tabanlı güvenlik araçları gibi yöntemlerin bu tehditlere karşı etkili çözümler sunduğu belirtilmiştir (Hashizume vd., 2013). Ancak, bu yöntemlerin etkinliği, kullanılan bulut modeline (Örneğin, genel, özel veya hibrit bulut) ve tehdit türüne bağlı olarak değişiklik gösterebilmektedir (Kshetri, 2013). Ayrıca, "Zero Trust Architecture" (Sıfır güven mimarisi) gibi modern yaklaşımlar, veri güvenliğini daha kapsamlı bir şekilde ele almayı hedeflemektedir (Kindervag, 2010).

Bu çalışmada, bulut bilişimde veri güvenliğiyle ilgili mevcut sorunlar ve bu sorunlara yönelik çözüm yöntemleri literatür taraması yöntemiyle incelenmiştir. Bulut bilişim teknolojisinin giderek artan kullanımı, güvenlik konusunu hem bireyler hem de kurumlar için kritik bir öncelik haline getirmiştir. Veri gizliliği, erişim kontrolü, kimlik doğrulama, siber saldırılara karşı korunma ve veri kaybının önlenmesi gibi güvenlik konuları, bulut tabanlı sistemlerde üzerinde durulması gereken temel sorunlar arasında yer almaktadır. Çalışmada, bu sorunların sadece teknik boyutu değil, aynı zamanda etik ve organizasyonel boyutları da ele alınmıştır.

Çalışmanın temel amacı, mevcut literatür ışığında bulut bilişim güvenliğinin kritik noktalarını belirlemek, bu bağlamda güncel sorunları sistematik bir şekilde sınıflandırmak ve bu sorunlara yönelik çözüm önerilerini sunmaktır. Özellikle, şifreleme teknikleri, kimlik ve erişim yönetimi, güvenlik protokolleri ve yapay zekâ tabanlı tehdit tespit sistemleri gibi güncel çözüm yöntemlerinin etkinliği değerlendirilmektedir. Bununla birlikte, çalışma, yalnızca mevcut durumu analiz etmekle kalmayıp, aynı zamanda gelecekteki araştırmalara rehberlik edecek stratejik öneriler sunmayı da amaçlamaktadır.

Böylelikle hem akademik literatüre hem de uygulamalı çalışmalara katkı sağlanarak, bulut bilişimde güvenliğin artırılmasına yönelik yeni bakış açıları geliştirilmesi hedeflenmektedir. Bu kapsamda, çalışma, güvenlik açıklarının en aza indirilmesi ve kullanıcıların bulut bilişim teknolojilerine duyduğu güvenin artırılmasına yönelik kapsamlı bir yol haritası oluşturmayı hedeflemektedir.

2. MATERYAL ve YÖNTEM

Bu çalışma, bulut bilişimde veri güvenliğiyle ilgili güncel sorunlar ve çözüm yöntemlerini inceleyen bir literatür taramasıdır. Literatür taraması, belirli bir konuyla ilgili mevcut akademik çalışmaların sistematik bir şekilde toplanması, analiz edilmesi ve sentezlenmesi yöntemiyle gerçekleştirilmiştir. Bu yöntemin temel amacı, bulut bilişimde veri güvenliğini etkileyen faktörleri anlamak ve bu alandaki mevcut bilgi birikimini değerlendirmektir (Fink, 2019).

Literatür taraması kapsamında, bulut bilişim, veri güvenliği, şifreleme, kimlik doğrulama, erişim kontrolü ve siber güvenlik gibi anahtar terimler kullanılarak çeşitli akademik veri tabanlarında arama yapılmıştır. Veri tabanı olarak Google Scholar, IEEE, ScienceDirect ve SpringerLink gibi güvenilir akademik kaynaklar tercih edilmiştir. Çalışma, 2000 yılından günümüze kadar yayımlanan makaleler ve raporları kapsamaktadır. Literatür taramasında özellikle, bulut bilişimdeki güvenlik açıkları, bu açıkları giderme yöntemleri ve gelecekteki olası güvenlik trendleri üzerine odaklanan çalışmalara yer verilmiştir (Kitchenham, 2004).

Bu çalışmada incelenecek akademik kaynaklar şu kriterlere göre seçilmiştir:

Anahtar Terimler: Çalışmalar, bulut bilişim, veri güvenliği, şifreleme, kimlik doğrulama, güvenlik protokolleri ve yapay zekâ gibi terimleri içermelidir.

Yayın Tarihi: Çalışmalar, 2000 yılından itibaren yayımlanmış ve güncel veri güvenliği tehditlerini ele almış olmalıdır (Torraco, 2005).

Metodoloji: Literatür taramasına dâhil edilen çalışmalar, bulut bilişimde veri güvenliğine dair teorik veya ampirik araştırmaları içermelidir.

Yayın Türü: Hakemli dergilerde yayımlanan, bilimsel geçerliliği olan akademik çalışmalar tercih edilmiştir (Booth vd., 2012).

Veri analizi, seçilen çalışmaların tematik analiz yöntemiyle gerçekleştirilmiştir (Braun ve Clarke, 2006). Bu analiz sürecinde, çalışmaların bulut bilişimde veri güvenliği ile ilgili bulguları detaylı bir şekilde değerlendirilmiş ve güvenlik sorunları ile çözüm yöntemleri tematik olarak sınıflandırılmıştır. Çalışma sonunda, bulut bilişimde veri güvenliğini sağlamaya yönelik mevcut yaklaşımlar, bu alandaki zorluklar ve gelecekte yapılabilecek çalışmalar için çıkarımlar sunulmuştur.

3. LİTERATÜR TARAMASI

Bulut bilişim teknolojisi, veri depolama ve iş süreçlerinde sağladığı esneklik, maliyet etkinliği ve ölçeklenebilirlik avantajlarıyla modern dijital ekosistemin temel bileşenlerinden biri haline gelmiştir (Armbrust vd., 2010). Ancak, bulut bilişim hizmetlerine olan talebin artması, veri güvenliği, mahremiyet ve düzenleyici uyum gibi kritik sorunları da beraberinde getirmiştir (Zissis ve Lekkas, 2012). Bu bağlamda, literatürde bulut bilişimde veri güvenliğiyle ilgili çeşitli sorunlar ve bu sorunlara yönelik çözüm önerileri geniş çapta ele alınmıştır (Subashini ve Kavitha, 2011).

Bu bölümde, bulut bilişim ve veri güvenliği ile ilgili yapılan akademik çalışmaların bir derlemesi sunulmaktadır. Literatür taramasında, bulut bilişim teknolojisinin tarihsel gelişimi, mevcut güvenlik tehditleri ve bu tehditlere yönelik çözüm yaklaşımları sistematik bir şekilde incelenmiştir. Ayrıca, güvenlik protokolleri, şifreleme yöntemleri, kimlik doğrulama mekanizmaları ve yapay zekâ tabanlı tehdit algılama sistemleri gibi yenilikçi uygulamalar değerlendirilmiştir (Hashizume vd., 2013). Bununla birlikte, çalışmada güncel eğilimler ve gelecekte yapılabilecek araştırmalara ışık tutacak öneriler de ele alınarak kapsamlı bir çerçeve oluşturulmuştur (Kshetri, 2013).

3.1. Bulut Bilişimin Tanımı ve Gelişimi

Bulut bilişim, kullanıcıların bilgi işlem kaynaklarına internet üzerinden erişmesini sağlayan bir hizmet modeli olarak tanımlanabilir. Bu teknoloji, altyapı, platform ve yazılım hizmetlerini ölçeklenebilir ve esnek bir şekilde sunarak bireylerin ve kurumların bilgi işlem ihtiyaçlarını karşılar (Mell ve Grance, 2011). Bulut bilişimin temel özelliği, kullanıcıların fiziksel donanım ve yazılım altyapılarına yatırım yapma gereksinimini ortadan kaldırması ve bunun yerine bu kaynakları bir hizmet olarak sunmasıdır. Bu yaklaşım, maliyet tasarrufu, ölçeklenebilirlik ve esneklik gibi avantajlar sunarak modern iş dünyasında hızla benimsenmiştir (Armbrust vd., 2010).

Bulut bilişim teknolojisinin gelişimi, bilgi işlem alanındaki önemli dönüm noktalarıyla şekillenmiştir. 1960'larda John McCarthy'nin "bilgi işlemin bir kamu hizmeti olarak sunulabileceği" fikri, bulut bilişimin temelini oluşturmuştur. 1990'ların sonlarında internetin yaygınlaşması ve veri merkezlerinin gelişimiyle birlikte, bulut bilişim daha uygulanabilir hale gelmiştir (Carr, 2008). 2000'lerin başında Amazon Web Services (AWS) gibi büyük şirketlerin bulut hizmetlerini piyasaya sürmesi, bu teknolojinin ticari olarak geniş ölçekte benimsenmesini sağlamıştır. Günümüzde ise Microsoft Azure, Google Cloud Platform ve IBM Cloud gibi hizmet sağlayıcılar, bulut bilişim pazarında lider konumdadır (Amazon Web Services, 2024).

Bulut bilişimin gelişim süreci boyunca, teknolojik altyapıların yanı sıra güvenlik ve mahremiyet konuları da önemli bir odak noktası haline gelmiştir. Verilerin internet üzerinden aktarılması, depolanması ve işlenmesi, kullanıcılar için büyük esneklik ve erişim kolaylığı sağlasa da, bu durum beraberinde çeşitli güvenlik risklerini de getirmiştir. Özellikle, hassas verilerin üçüncü taraf sağlayıcıların altyapılarında tutulması, veri ihlalleri, yetkisiz erişimler ve siber saldırılar gibi sorunları daha da görünür hale getirmiştir (Zissis ve Lekkas, 2012). Ayrıca, veri depolama ve işleme süreçlerinde mahremiyetin korunması, yasal düzenlemeler ve uluslararası standartlarla daha fazla ilişkilendirilerek çözüm arayışlarını artırmıştır (Hashizume vd., 2013).

Literatürde, bulut bilişimin hızla gelişen bir teknoloji olduğu ve iş süreçlerini dönüştürme potansiyeline sahip olduğu vurgulanmaktadır. Özellikle, bu teknolojinin işletmelere maliyet etkinliği, operasyonel esneklik ve hız kazandırdığı belirtilmiştir (Armbrust vd., 2010). Bununla birlikte, güvenlik ve mahremiyetle ilgili endişeler, bu teknolojinin benimsenme sürecini yavaşlatan önemli faktörler arasında yer almıştır. Örneğin, veri ihlali vakalarının sayısının artması ve kullanıcıların mahremiyet konusundaki farkındalığının yükselmesi hem bulut sağlayıcılarını hem de kullanıcıları daha güçlü güvenlik çözümleri geliştirmeye yönlendirmiştir (Rittinghouse ve Ransome, 2010).

Gelecekte, bulut bilişim teknolojisinin yalnızca iş dünyasında değil, eğitim, sağlık ve kamu hizmetleri gibi sektörlerde de daha yaygın bir şekilde kullanılacağı öngörülmektedir. Ancak, bu genişleme sürecinde, teknolojinin güvenlik açıklarının ve mahremiyetle ilgili endişelerin giderilmesi büyük önem taşımaktadır. Blockchain, yapay zekâ tabanlı güvenlik sistemleri ve kuantum şifreleme gibi yenilikçi çözümler, bulut bilişimde güvenlik seviyesini artırmada potansiyel olarak önemli bir rol oynayacaktır (Kshetri, 2013). Bu bağlamda, literatür, bulut bilişimde güvenlik ve mahremiyet konularının gelecekteki teknolojik yenilikler ve düzenleyici çerçevelerle daha da gelişeceğine işaret etmektedir.

3.2. Bulut Bilişim Modelleri

Bulut bilişim, hizmet sunumunun türüne ve dağıtım şekline bağlı olarak farklı modellerden oluşmaktadır. National Institute of Standards and Technology (NIST) tarafından yapılan tanımlamalara göre bulut bilişim modelleri genellikle iki ana kategoride incelenmektedir. NIST, Amerika Birleşik Devletleri Ticaret Bakanlığı'na bağlı bir kurumdur. 1901 yılında kurulmuş olan NIST, bilimsel araştırmalar ve teknik standartların geliştirilmesi için faaliyet gösteren önemli bir enstitüdür. NIST'in belli başlı görevleri şöyle özetlenebilir; Standartların geliştirilmesi, teknolojik gelişimi destekleme, siber güvenlik alanında, şifreleme standartları ve güvenlik politikaları gibi rehberlik belgeleri yayımlama. NIST'in belirlemiş olduğu iki ana kategori: Hizmet Modelleri ve Dağıtım Modelleri (Mell ve Grance, 2011).

NIST, bulut bilişim alanında da önemli bir role sahiptir. 2011 yılında yayımladığı "The NIST Definition of Cloud Computing" adlı belge, bulut bilişimin tanımlanmasında ve anlaşılmasında küresel bir standart oluşturmuştur. Bu belgede bulut bilişim:

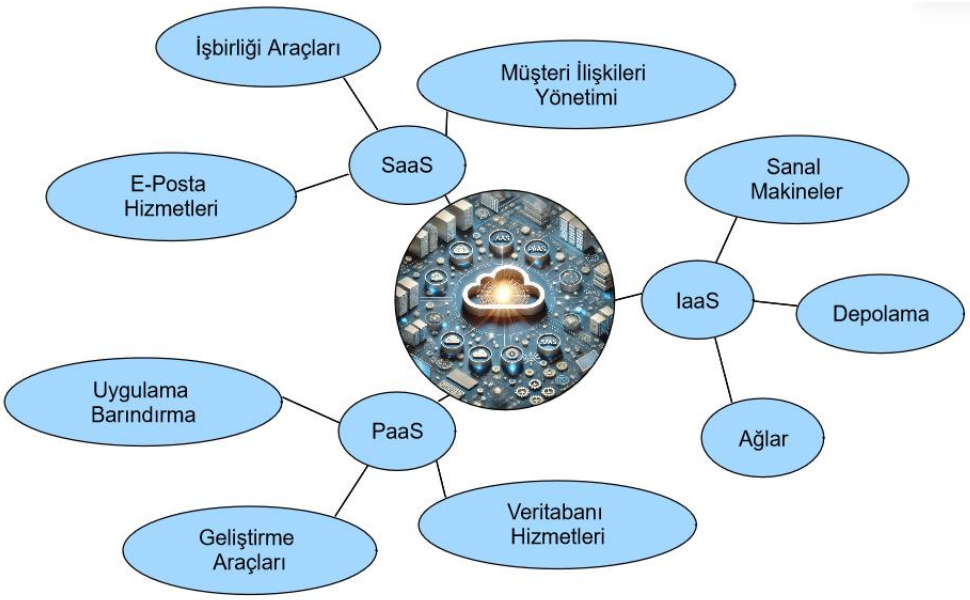
- Hizmet Modelleri (IaaS, PaaS, SaaS),
- Dağıtım Modelleri (Özel, Ortak, Hibrit, Topluluk),
- Ve özellikleri (Talep üzerine hizmet, geniş ağ erişimi, kaynak havuzu, hızlı esneklik, ölçümlenebilir hizmet) ile kapsamlı bir şekilde tanımlanmıştır (Mell ve Grance, 2011).

3.2.1. Hizmet Modelleri

Hizmet modelleri, bulut bilişim hizmetlerinin kullanıcıya hangi düzeyde sağlandığını ve hangi kapsamda erişim sağladığını açıklayan bir sınıflamadır. Bu sınıflama, bulut bilişim altyapısının kullanıcılar tarafından ne ölçüde kontrol edilebildiği ve yönetilebildiği gibi kriterlere dayanır. Hizmet modelleri, kullanıcıların yalnızca ihtiyaç duydukları hizmet seviyesini seçmelerine imkân tanırken, aynı zamanda kaynakların etkili bir şekilde kullanılmasını sağlar. Genel olarak üç temel kategoriden oluşur:

- **Altyapı Hizmeti Olarak Bulut (Infrastructure as a Service - IaaS)**
  IaaS, kullanıcılara temel bilgi işlem altyapısı hizmetlerini sağlar. Sanal sunucular, depolama alanları ve ağ kaynakları bu modele dahildir. Kullanıcılar bu hizmeti kullanarak fiziksel donanım yatırımı yapmaksızın kaynaklarını ölçeklendirme esnekliği kazanırlar (Mell ve Grance, 2011).
- **Platform Hizmeti Olarak Bulut (Platform as a Service - PaaS)**
  PaaS modeli, yazılım geliştirme ve dağıtım için gerekli platformları sağlar. Bu modelde kullanıcılar, sunucuların yönetimiyle ilgilenmeden yazılım geliştirme süreçlerini hızlandırabilirler (Armbrust vd., 2010). Örneğin, Google App Engine ve Microsoft Azure bu modelin popüler örneklerindendir.
- **Yazılım Hizmeti Olarak Bulut (Software as a Service - SaaS)**
  SaaS, son kullanıcıların yazılımı doğrudan internet üzerinden kullanmalarını sağlar. Bu modelde yazılım, sağlayıcı tarafından yönetilir ve kullanıcıların yalnızca bir internet bağlantısına ihtiyaçları vardır. Gmail (https://www.gmail.com), Microsoft Office 365 (https://www.office.com) ve Salesforce (https://www.salesforce.com) bu kategoriye örnek olarak verilebilir (Zhang vd., 2010).

Bu kategoriler, kullanıcıların altyapıyı doğrudan yönetmelerinden, yalnızca bir yazılım uygulamasını kullanmalarına kadar geniş bir esneklik sunar. Örneğin, IaaS modelinde kullanıcılar sanal makineler veya depolama alanı gibi temel altyapı hizmetlerine erişirken, PaaS modelinde yazılım geliştirme için gerekli platform hizmetlerini kullanabilirler. SaaS modeli ise, kullanıcıların yazılım uygulamalarını internet üzerinden doğrudan kullanmalarına imkân tanır ve bu süreçte altyapıyı veya platformu yönetme gerekliliğini ortadan kaldırır. Bu çeşitlilik, bulut bilişim hizmetlerinin farklı kullanıcı ihtiyaçlarına uyum sağlamasını mümkün kılar (Mell ve Grance, 2011).



Şekil 1. Bulut Bilişim Hizmet Modeli Örnek Uygulamaları (Kaynak: Yazar)

3.2.2. Dağıtım Modelleri

Bulut bilişim dağıtım modelleri, bulut hizmetlerinin kullanıcıya hangi yapılandırma veya erişim yöntemiyle sunulduğunu ifade eder. Bu modeller, hizmetlerin ne şekilde erişilebilir olduğunu, hangi kullanıcı gruplarına yönelik tasarlandığını ve veri güvenliği, gizlilik gibi faktörleri nasıl ele aldığını belirlemek için kritik öneme sahiptir. Dağıtım modelleri, işletmelerin ihtiyaçlarına ve operasyonel gereksinimlerine uygun bir bulut stratejisi geliştirmesine imkân tanır. NIST tarafından yapılan tanımlamalara göre bulut bilişim dağıtım modelleri dört ana başlıkta incelenmektedir: özel bulut, ortak bulut, hibrit bulut ve topluluk bulutu (Mell ve Grance, 2011).

1. Özel Bulut (Private Cloud): Özel bulut, yalnızca bir kuruluşun kullanımına özel olarak ayrılmış bir altyapıdır. Genellikle büyük ölçekli işletmelerin tercih ettiği bu modelde veri güvenliği ve gizlilik ön plandadır (Marinos ve Briscoe, 2009).
2. Ortak Bulut (Public Cloud): Ortak bulut, genellikle birden fazla kuruluşun aynı altyapıyı paylaştığı bir modeldir. Bu model, maliyet etkinliği nedeniyle küçük ve orta ölçekli işletmeler tarafından tercih edilmektedir (Buyya vd., 2009).
3. Hibrit Bulut (Hybrid Cloud): Hibrit bulut modeli, özel ve ortak bulut altyapılarının bir kombinasyonudur. Bu model, işletmelere esneklik ve maliyet avantajı sağlarken, hassas verilerin özel bulut ortamında tutulmasını mümkün kılar (Gonzalez vd., 2012).
4. Topluluk Bulutu (Community Cloud): Topluluk bulutu, belirli bir sektöre veya topluluğa yönelik altyapı hizmetlerinin paylaşıldığı bir modeldir. Örneğin, sağlık veya eğitim sektörü için geliştirilen bulut sistemleri bu modele dahildir (Marinos ve Briscoe, 2009).

Bu modellerin her biri, kullanıcı ihtiyaçlarına ve iş gereksinimlerine göre belirli avantajlar ve sınırlamalar sunmaktadır. Örneğin, özel bulut, yüksek düzeyde veri güvenliği ve özelleştirilebilirlik sağlaması nedeniyle, özellikle finansal hizmetler, sağlık sektörü ve devlet kurumları gibi hassas verilerle çalışan kuruluşlar tarafından tercih edilmektedir. Bu model, işletmelerin verilerini kendi bünyelerinde saklayarak tam kontrol sahibi olmalarına olanak tanır, ancak aynı zamanda yüksek altyapı maliyetleri ve yönetim gereksinimleri gibi dezavantajlara sahiptir. Buna karşılık, ortak bulut, altyapının birden fazla kullanıcı veya kuruluş arasında paylaşılması sayesinde düşük maliyetli bir çözüm sunar. Bu model, küçük ve orta ölçekli işletmeler için idealdir, ancak veri gizliliği ve güvenlik konularında bazı riskler barındırabilir.

Hibrit bulut, özel ve ortak bulutların avantajlarını bir araya getirerek, işletmelere her iki dünyanın da en iyisini sunar. Hassas verilerin özel bulut ortamında tutulması, operasyonel esneklik ve maliyet avantajları için ortak bulut kaynaklarının kullanılması, bu modeli cazip hale getirmektedir. Özellikle değişken iş yüklerine sahip olan veya sezonluk taleplerle karşılaşan işletmeler için hibrit bulut çözümleri büyük bir esneklik sağlar. Son olarak, topluluk bulutu, belirli bir sektöre veya topluluğa özel ihtiyaçlara yönelik tasarlanmış bir modeldir. Örneğin, eğitim sektöründe üniversiteler arası iş birliği veya sağlık sektöründe

veri paylaşımı gibi durumlarda topluluk bulutları, kullanıcıların ortak amaçlarına hizmet eden özelleştirilmiş bir altyapı sunar.

Bu dağıtım modelleri, işletmelere stratejik bir esneklik sağlarken, veri güvenliği, maliyet yönetimi ve operasyonel verimlilik gibi konularda farklı seçenekler sunar. Hangi modelin seçileceği, işletmenin öncelikleri, büyüklüğü, bütçesi ve uzun vadeli hedefleri gibi faktörlere bağlıdır.

Aşağıda bulut dağıtım modellerini kullanan küresel bazı şirketlerden örnek bilgiler bulunmaktadır.

Özel Bulut (Private Cloud)

- Amazon Virtual Private Cloud (Amazon VPC): Amazon'un özel bulut çözümü, kuruluşların kendi izole edilmiş bulut ortamlarını oluşturmasına imkân tanır (Amazon Vpc, 2024).
- VMware vSphere Private Cloud: VMware tarafından sunulan bir çözüm, kuruluşların kendi veri merkezlerinde özel bir bulut altyapısı kurmasını sağlar (Vmware, 2024).
- Microsoft Azure Stack: Azure hizmetlerinin kendi veri merkezinizde çalıştırılmasına imkân veren özel bir bulut çözümüdür (Azure Stack, 2024).

Ortak Bulut (Public Cloud)

- Amazon Web Services (AWS): Dünyanın en popüler ortak bulut hizmet sağlayıcılarından biri olup IaaS, PaaS ve SaaS gibi hizmetler sunar (AWS, 2024).
- Google Cloud Platform: Google'ın altyapısında barındırılan ve çok çeşitli bulut hizmetleri sunan bir ortak bulut çözümüdür (GCP, 2024).
- Microsoft Azure: Microsoft'un ortak bulut platformu, küresel veri merkezlerinde ölçeklenebilir hizmetler sağlar (Azure, 2024).

Hibrit Bulut (Hybrid Cloud)

- Microsoft Azure Arc: Hem Azure veri merkezlerini hem de yerel altyapıyı yönetmeyi sağlayan hibrit bir çözüm (Azure Arc, 2024).
- IBM Hybrid Cloud: IBM'in hibrit bulut çözümü hem yerel sistemlerle hem de bulut ortamıyla entegre çalışmayı destekler (IBM Cloud, 2024).
- Google Anthos (https://cloud.google.com/anthos): Google'ın, hibrit bulutlar ve çoklu bulut ortamları için bir çözümüdür.

Topluluk Bulutu (Community Cloud)

- OpenStack (https://www.openstack.org): Açık kaynaklı bir topluluk bulut platformu olup, genellikle belirli sektörler veya ortak projeler için kullanılır.
- CERN Cloud: Avrupa Nükleer Araştırma Merkezi'nin (CERN) bilimsel araştırmalar için oluşturduğu topluluk bulut örneğidir (CERN Cloud, 2024).
- California Community Colleges Cloud: Kaliforniya'daki topluluk kolejleri için oluşturulan, eğitim odaklı bir topluluk bulut çözümüdür (California Community Colleges Cloud, 2024).

3.3. Bulut Bilişimde Veri Güvenliği Sorunları

Bulut bilişim, işletmeler ve bireyler için depolama, işlem gücü ve yazılım hizmetleri gibi birçok avantaj sunarken, veri güvenliği konusunda önemli endişeleri de beraberinde getirmektedir. Bulut ortamında veriler, geleneksel yöntemlerden farklı olarak uzak sunucularda depolandığından, kullanıcılar üzerinde tam kontrole sahip olmadıkları bir altyapıya güvenmek zorunda kalırlar. Bu durum, veri ihlalleri, yetkisiz erişim ve kimlik doğrulama açıkları gibi çeşitli güvenlik tehditlerine yol açabilir (Mell ve Grance, 2011). Ayrıca, veri bütünlüğü ve gizliliği gibi kritik unsurların korunması, bulut hizmet sağlayıcılarının sunduğu güvenlik protokollerine bağlıdır (Subashini ve Kavitha, 2011). Özetle, bulut bilişim teknolojisinin hızlı benimsenmesi, beraberinde veri güvenliğine yönelik daha sofistike tehditler ve çözüm arayışlarını getirmiştir. Bu bağlamda, veri güvenliği sorunları incelendiğinde, güvenlik açıkları, kimlik doğrulama eksiklikleri, veri kaybı riskleri ve düzenlemelere uyumluluk gibi çeşitli alt başlıklar öne çıkmaktadır (Ristenpart vd., 2009).

3.3.1. Veri Güvenliği Açıkları ve Saldırılar

Bulut bilişim ortamında veri güvenliği, saldırganların hedef aldığı en kritik unsurlar arasında yer almaktadır. Bulut altyapısının doğası gereği, veriler genellikle birçok farklı fiziksel ve sanal katmanda işlenir, bu da saldırganların çeşitli noktaları hedef almasına olanak tanır. Özellikle, bulut sağlayıcıları tarafından sunulan hizmetlerde meydana gelen güvenlik açıkları, kullanıcı verilerinin yetkisiz erişimlere ve siber saldırılara karşı savunmasız hale gelmesine yol açabilir. Bu tür açıklar, saldırganların hassas bilgilere erişmesini, bu bilgileri değiştirmesini veya tamamen silmesini mümkün kılabilir.

Bu bağlamda, OWASP (Open Web Application Security Project) tarafından yayımlanan güncel güvenlik tehditleri listesi, veri güvenliği açıklarını anlamak ve bu açıklarla mücadele etmek için önemli bir rehber sunmaktadır.

Tablo 1. OWASP 2024 Güncel Güvenlik Riskleri ve Açıklamaları (Owasp, 2024)

Sıra	Güvenlik Riski	Açıklama
M1	Hatalı Kimlik Bilgisi Kullanımı	Zayıf şifreler, yanlış saklanan kimlik bilgileri veya yetersiz kimlik doğrulama mekanizmaları.
M2	Yetersiz Tedarik Zinciri Güvenliği	Tedarik zincirindeki üçüncü taraf hizmetlerdeki güvenlik açıkları nedeniyle sistemlerin tehlikeye girmesi.
M3	Güvensiz Kimlik Doğrulama/Yetkilendirme	Eksik veya yanlış uygulanan kimlik doğrulama ve yetkilendirme süreçleri nedeniyle yetkisiz erişim.
M4	Yetersiz Girdi/Çıktı Doğrulaması	Kullanıcı girişlerinin veya sistem çıktılarının yeterince doğrulanmaması, enjeksiyon saldırıları gibi riskler.
M5	Güvensiz İletişim	Veri aktarımında kullanılan yetersiz şifreleme protokolleri nedeniyle hassas bilgilerin ele geçirilmesi.
M6	Yetersiz Gizlilik Kontrolleri	Hassas verilerin uygun şekilde korunmaması sonucu veri ihlalleri yaşanması.
M7	Yetersiz İkili Koruma	Kod veya yazılım bileşenlerinin manipülasyona karşı yeterince korunmaması, saldırganların sistemi kötüye kullanması.
M8	Güvenlik Yanlış Yapılandırmaları	Sistem yapılandırmalarındaki hatalar veya eksiklikler nedeniyle güvenlik açıklarının oluşması.
M9	Güvensiz Veri Depolama	Veri depolamada kullanılan şifreleme veya güvenlik önlemlerinin yetersizliği sonucu veri ihlalleri.
M10	Yetersiz Kriptografi	Şifreleme algoritmalarının yanlış uygulanması veya yetersiz düzeyde olması nedeniyle veri güvenliğinin ihlal edilmesi.

OWASP'ın bulut bilişim ve web uygulamaları için belirlediği güvenlik riskleri, veri güvenliğini tehdit eden temel açıkları içermektedir. 2024 tehdit listesi ve 2016 yılındaki tehdit listesi aşağıdaki tabloda karşılaştırılmıştır. Değişim aradan geçen 8 yılda güvenlik tehditlerinin değişikliğe uğradığı görülmektedir.

Tablo 2. OWASP 2024 Güncel Güvenlik Riskleri ve 2016 Listesi ile Karşılaştırması (Owasp, 2024)

OWASP-2016	OWASP-2024-Sürümü	2016 ve 2024 Karşılaştırması
M1: Hatalı Platform Kullanımı	M1: Hatalı Kimlik Bilgisi Kullanımı	Yeni
M2: Güvensiz Veri Depolama	M2: Yetersiz Tedarik Zinciri Güvenliği	Yeni
M3: Güvensiz İletişim	M3: Güvensiz Kimlik Doğrulama / Yetkilendirme	M4 ve M6'nın M3 ile birleştirilmesi
M4: Güvensiz Kimlik Doğrulama	M4: Yetersiz Girdi/Çıktı Doğrulaması	Yeni
M5: Yetersiz Kriptografi	M5: Güvensiz İletişim	M3'ten M5'e taşındı
M6: Güvensiz Yetkilendirme	M6: Yetersiz Gizlilik Kontrolleri	Yeni
M7: İstemci Kod Kalitesi	M7: Yetersiz İkili Koruma	M8 ve M9'un M7 ile birleştirilmesi
M8: Kod Manipülasyonu	M8: Güvenlik Yanlış Yapılandırmaları	M8'in yeniden yazılması [M10'dan taşındı]
M9: Tersine Mühendislik	M9: Güvensiz Veri Depolama	M2'den M9'a taşındı
M10: Ek İşlevsellik	M10: Yetersiz Kriptografi	M5'ten M10'a taşındı

Tablo 2'yi şöyle açıklayabiliriz; OWASP'ın 2024 güncellenmiş listesi, önceki yıllara kıyasla daha geniş bir güvenlik perspektifi sunarak hem mevcut hem de yeni tehditleri ele almıştır. 2016 listesindeki bazı tehditler yeni kategorilerle genişletilirken, bazıları birleştirilmiş ya da yeniden düzenlenmiştir. Örneğin, "Hatalı Kimlik Bilgisi Kullanımı" ve "Yetersiz Tedarik Zinciri Güvenliği" gibi yeni başlıklar, modern sistemlerdeki risklere dikkat çekerken, "Güvensiz Kimlik Doğrulama" ve "Güvensiz Yetkilendirme" başlıkları birleştirilerek "Güvensiz Kimlik Doğrulama/Yetkilendirme" altında toplanmıştır. Ayrıca, "Yetersiz Kriptografi" ve "Güvensiz Veri Depolama" gibi tehditler önceki yerlerinden taşınarak güncel tehdit algısıyla daha uygun bir şekilde yeniden kategorize edilmiştir. Liste, yeni tehditler arasında "Yetersiz Girdi/Çıktı Doğrulaması" ve "Yetersiz Gizlilik Kontrolleri" gibi konuları ele alarak, veri güvenliği ve sistem dayanıklılığı açısından kapsamlı bir yaklaşım sunmaktadır. Bu güncellemeler, modern uygulamalarda karşılaşılan tehditleri daha etkili bir şekilde tanımlamak ve önlem almak için rehber niteliğindedir.

Veri ihlalleri, bulut bilişim kullanıcılarının en sık karşılaştığı sorunlardan biridir ve bu ihlaller genellikle zayıf kimlik doğrulama mekanizmaları, yetersiz şifreleme yöntemleri veya yanlış yapılandırılmış bulut hizmetleri sonucunda ortaya çıkar (Subashini ve Kavitha, 2011). Örneğin, kullanıcıların zayıf şifreler kullanması veya sistemlerin varsayılan güvenlik ayarlarında bırakılması, saldırganların bu sistemlere kolayca erişmesine neden olabilir. Aynı şekilde, bulut hizmet sağlayıcılarının güvenlik güncellemelerini zamanında yapmaması, veri ihlali riskini artırmaktadır.

Bunun yanı sıra, hizmet reddi saldırıları (DDoS: Distrubuted Denial of Service Attack), bulut altyapısına yönelik sıklıkla kullanılan bir başka saldırı türüdür. Bu tür saldırılarda, birden fazla kaynaktan gelen yoğun trafik, sistem kaynaklarının aşırı yüklenmesine ve hizmetlerin geçici olarak devre dışı kalmasına neden olur (Ristenpart vd., 2009). DDoS saldırıları yalnızca hizmet kesintilerine yol açmakla kalmaz, aynı zamanda veri güvenliği açıklarını tetikleyerek saldırganların sistemlere sızmasına olanak tanıyabilir. Örneğin, bu tür saldırılar sırasında ortaya çıkan karışıklık, saldırganların sistemdeki diğer zayıflıkları sömürmesini kolaylaştırabilir.

Bulut hizmet sağlayıcıları ve internet altyapı şirketleri, dağıtılmış hizmet reddi (DDoS) saldırılarının hedefi olmuştur. DDoS saldırısına yakın tarihlerde örnek vermek gerekirse Cloudflare verilebilir. Cloudflare, web sitelerinin performansını artırmak ve güvenliğini sağlamak amacıyla hizmetler sunan bir Amerikan teknoloji şirketidir. 2009 yılında kurulan şirket, içerik dağıtım ağı, DDoS koruması, internet güvenliği ve alan adı sunucusu hizmetleri gibi çeşitli çözümler sunmaktadır (Cloudflare, 2024). Eylül 2024'te Cloudflare, saniyede 2 milyardan fazla paket ve 3 Tbps'yi aşan hacimlere ulaşan 100'den fazla "hiper-volumetrik L3/4 DDoS saldırısını" engellediğini bildirmiştir. Bu saldırılar, özellikle finansal hizmetler, telekomünikasyon ve internet sektörlerini hedef almıştır (Cyberwebeyeos, 2024).

Bu güvenlik sorunları hem bireysel kullanıcıların hem de işletmelerin verilerini güvence altına almak için daha gelişmiş güvenlik önlemleri almasını zorunlu kılmaktadır. Güvenli kimlik doğrulama, veri şifreleme, düzenli güvenlik güncellemeleri ve siber tehdit izleme sistemleri, bu tür saldırılara karşı etkili önlemler arasında yer almaktadır. Ancak, saldırganların yöntemlerini sürekli geliştirmesi, bulut ortamında veri güvenliğinin sürekli bir meydan okuma olarak kalmasını sağlamaktadır.

Bunun yanı sıra, yan kanal saldırıları (Side Channel Attack), özellikle paylaşımlı bulut altyapılarında sıkça görülen bir güvenlik sorunudur. Yan kanal saldırıları, bir sistemin doğrudan tasarımından veya algoritmalarından ziyade, sistemin çalışması sırasında ürettiği fiziksel veya davranışsal bilgilerden yararlanmayı amaçlayan saldırı türleridir. Bu saldırılar, özellikle paylaşılan bulut ortamlarında büyük bir tehdit oluşturur. Saldırganlar, bir sistemin CPU kullanımı, güç tüketimi, zamanlama bilgileri ya da ağ trafiği gibi yan kanallarını analiz ederek hassas bilgilere erişmeye çalışır. Bulut bilişimde, yan kanal saldırıları genellikle paylaşılan altyapılar nedeniyle gerçekleşir. Birden fazla müşteri, aynı fiziksel sunucuyu kullandığında, saldırganlar, bu paylaşılan kaynaklardan bilgi sızıntılarını gözlemleyebilir ve kurbanın işlem detaylarını analiz edebilir (Zhang vd., 2010). Örneğin, sanallaştırma teknolojileri aracılığıyla birden fazla kullanıcı aynı fiziksel sunucuyu paylaştığında, saldırganlar, CPU (Central Processing Unit), bellek veya ağ kaynaklarındaki bilgi sızıntılarını kullanabilir (Ristenpart vd., 2009).

Veri güvenliği açıkları, yalnızca dış tehditlerden değil, aynı zamanda iç tehditlerden de kaynaklanabilir. Bulut hizmet sağlayıcılarının personelinin yetkisiz erişimi veya kullanıcıların bilinçsiz davranışları, veri bütünlüğünü ve gizliliğini tehlikeye atabilir. Özetle, veri güvenliği açıkları ve saldırılar hem kullanıcılar hem de hizmet sağlayıcılar için sürekli bir risk oluşturmakta ve bu risklerin minimize edilmesi için güçlü güvenlik politikalarının uygulanmasını gerektirmektedir.

3.3.2. Kimlik Doğrulama ve Erişim Kontrolü Sorunları

Bulut bilişim ortamında güvenliğin temel taşlarından biri, kimlik doğrulama ve erişim kontrol mekanizmalarının etkin bir şekilde uygulanmasıdır. Bu mekanizmalar, yalnızca yetkili kullanıcıların verilere ve hizmetlere erişmesini sağlamayı amaçlar. Ancak, bu alanda karşılaşılan eksiklikler ve tehditler, bulut bilişim kullanıcılarını veri ihlalleri ve yetkisiz erişimlere karşı savunmasız bırakmaktadır.

Kimlik doğrulama süreçlerinde kullanılan geleneksel yöntemler, genellikle zayıf şifre politikaları nedeniyle saldırganlar için kolay hedef haline gelir. Kullanıcıların güçlü ve benzersiz şifreler oluşturmayı ihmal etmesi veya aynı şifreyi birden fazla platformda kullanması, kimlik bilgilerinin çalınması riskini artırır. Özellikle, phishing saldırıları (Sahte e-posta, mesaj veya web siteleri ile verileri çalma) ve şifre tahmin saldırıları gibi yöntemler, kullanıcıların kimlik bilgilerini ele geçirmek için yaygın olarak kullanılır (Kanagasabapathi vd., 2016).

Erişim kontrolü sorunları da bulut bilişim ortamlarında ciddi bir güvenlik açığı oluşturmaktadır. Yanlış yapılandırılmış erişim izinleri, saldırganların hassas verilere yetkisiz erişim sağlamasına neden olabilir. Örneğin, paylaşılan depolama hizmetlerinde bir kullanıcının tüm verilerinin yanlışlıkla "herkese açık" olarak ayarlanması, veri sızıntısına yol açabilir. Bu tür durumlar, genellikle karmaşık erişim kontrol politikalarının doğru bir şekilde uygulanmamasından kaynaklanmaktadır (Subashini ve Kavitha, 2011).

Çok faktörlü kimlik doğrulama (MFA: Multi-Factor Authentication) eksikliği, kimlik doğrulama ve erişim kontrolüyle ilgili bir diğer kritik sorundur. MFA, kullanıcıların kimliklerini doğrulamak için birden fazla doğrulama faktörü kullanmasını gerektirir ve bu da saldırganların sistemlere sızmasını zorlaştırır. MFA, yalnızca bir şifre ile yetinmez, bunun yerine farklı kategorilerden gelen en az iki doğrulama unsuru ister:

1. Bildikleriniz: Şifre, PIN gibi kullanıcıya özgü bilgiler.
2. Sahip Olduklarınız: Akıllı telefon, güvenlik token'ı veya bir doğrulama uygulaması gibi fiziksel öğeler.
3. Biyometrik Özellikler: Parmak izi, yüz tanıma veya iris taraması gibi biyolojik doğrulama yöntemleri.

MFA, tek faktörlü doğrulamanın zayıflıklarını gidermeye yardımcı olarak yetkisiz erişim riskini önemli ölçüde azaltır. Örneğin, kullanıcı bir şifreyi kaybetse veya çaldırsa bile, diğer doğrulama faktörleri ek bir güvenlik katmanı sağlar. Ancak, birçok bulut sağlayıcısı veya kullanıcı, bu önemli güvenlik özelliğini uygulamayı ihmal etmektedir. Ayrıca, MFA kullanılsa bile, zayıf uygulamalar veya düşük kaliteli doğrulama yöntemleri nedeniyle bu sistemler bazen etkisiz kalabilir (Aloul ve El-Hajj, 2009).

Sonuç olarak, kimlik doğrulama ve erişim kontrolü sorunları hem bireysel kullanıcılar hem de işletmeler için büyük bir risk oluşturmaktadır. Bu sorunların üstesinden gelmek için güçlü şifre politikalarının benimsenmesi, erişim izinlerinin dikkatli bir şekilde yapılandırılması ve çok faktörlü kimlik doğrulama gibi ileri düzey güvenlik önlemlerinin uygulanması büyük önem taşımaktadır.

3.3.3. Veri Kaybı ve Yedekleme Zorlukları

Bulut bilişim ortamında veri kaybı, kullanıcılar ve işletmeler için ciddi riskler arasında yer almaktadır. Verilerin fiziksel sunucular yerine sanal ortamda depolanması, kayıplara karşı korunma süreçlerini daha karmaşık hale getirebilir. Veri kaybı, genellikle hatalı sistem güncellemeleri, insan hataları, siber saldırılar veya teknik arızalar gibi çeşitli nedenlerle meydana gelebilir. Özellikle, yetersiz yedekleme stratejileri ve yanlış yapılandırılmış sistemler, veri kaybı riskini artıran başlıca etmenler arasında yer almaktadır (Subashini ve Kavitha, 2011).

Veri kaybının en yaygın nedenlerinden biri, bulut sağlayıcılarının yaşadığı teknik arızalardır. Örneğin, sunucu çökmeleri, elektrik kesintileri veya depolama cihazlarındaki fiziksel hasarlar, bulutta tutulan verilere erişimi kesintiye uğratabilir. Ayrıca, siber saldırılar, özellikle fidye yazılımı (Ransomware: Verilerin arka plan yazılımları ile erişilemez hale getirilmesi ve karşılığında fidye talep edilmesi) saldırıları, kullanıcıların verilerini rehin alarak kayıplara yol açabilir. Bu tür durumlar, veri güvenliğinin yanı sıra veri bütünlüğünün de korunmasını gerektirir (Armbrust vd., 2010).

Yedekleme zorlukları, veri kaybını önlemenin temel bir yolu olmasına rağmen, bulut ortamında bu süreçler genellikle karmaşıktır. Yedekleme işlemlerinin zamanında yapılmaması, eksik veya hatalı yedeklemeler, kritik verilerin geri alınamamasına neden olabilir. Ayrıca, yedekleme sürecinin güvenli bir şekilde gerçekleştirilmemesi durumunda, veriler başka bir saldırıya açık hale gelebilir. Örneğin, yedeklerin uygun şekilde şifrelenmemesi durumunda, saldırganlar bu verilere kolayca erişebilir.

Veri kaybı ve yedekleme sorunlarının önlenmesi için kullanıcıların ve bulut sağlayıcılarının iş birliği içinde çalışması gereklidir. Kullanıcılar, verilerini düzenli olarak yedeklemek ve bu yedeklerin bütünlüğünü doğrulamak için etkili stratejiler geliştirmelidir. Bulut sağlayıcıları ise daha güvenilir yedekleme altyapıları, şifreleme mekanizmaları ve felaket kurtarma çözümleri sunarak bu süreçleri kolaylaştırabilir. Sonuç olarak, veri kaybını önlemek için etkili bir yedekleme stratejisinin yanı sıra proaktif güvenlik önlemleri de hayati öneme sahiptir.

Bulut bilişim ortamlarında veri kaybı, kullanıcılar ve kuruluşlar için kritik bir risk alanıdır. Verilerin uzak sunucularda saklanması, güvenlik açıklarının yanı sıra yedekleme süreçlerinde de karmaşıklıklara neden olmaktadır. Yanlış yapılandırılmış sistemler, insan hataları ve teknik arızalar, verilerin kalıcı olarak

kaybedilmesine yol açabilecek başlıca faktörlerdir. Özellikle, hizmet sağlayıcıların yedekleme stratejilerindeki eksiklikler, veri kaybının geri dönüşünü zorlaştırmaktadır (Barona ve Anita, 2017). Ayrıca, kullanıcıların yedekleme süreçlerine dair bilgi eksikliği ve bu işlemleri ihmal etmeleri, veri güvenliğini daha da savunmasız hale getirmektedir.

Siber saldırılar da veri kaybının önemli nedenlerinden biridir. Örneğin, fidye yazılımı (Ransomware) saldırıları sırasında veriler şifrelenerek erişilemez hale getirilmekte, bu da kritik verilere ulaşımı imkânsız kılmaktadır. Bu tür saldırılar, yalnızca verilerin güvenliğini değil, aynı zamanda organizasyonların iş sürekliliğini de tehdit etmektedir. Yedekleme süreçlerinde, şifreleme gibi ileri düzey güvenlik yöntemlerinin kullanılmaması, yedeklenen verilerin dahi tehdit altında olmasına yol açabilmektedir (Barona ve Anita, 2017).

Veri kaybı ve yedekleme sorunlarının önlenmesi için kullanıcıların düzenli ve güvenli yedekleme stratejileri oluşturması gereklidir. Aynı zamanda bulut hizmet sağlayıcılarının, daha güvenilir altyapılar sunarak kullanıcıların veri güvenliğine dair endişelerini gidermesi gerekmektedir. Etkili bir yedekleme sistemi hem fiziksel hem de siber tehditlere karşı verileri korumak için hayati öneme sahiptir.

3.3.4. Şifreleme ve Veri Gizliliği

Bulut bilişim ortamında şifreleme, veri gizliliğini korumanın en etkili yöntemlerinden biri olarak kabul edilmektedir. Şifreleme, verilerin yalnızca yetkili kullanıcılar tarafından okunabilir olmasını sağlamak için matematiksel algoritmalar kullanılarak dönüştürülmesini içerir. Bu yöntem hem verilerin bulut sunucularında depolanırken hem de veri aktarımı sırasında güvenliğini sağlamada kritik bir rol oynar (Barona ve Anita, 2017). Ancak, şifreleme teknolojilerinin etkili bir şekilde uygulanmaması veya zayıf şifreleme protokollerinin kullanılması, hassas bilgilerin yetkisiz kişiler tarafından ele geçirilmesine yol açabilir.

Asimetrik şifreleme (Örneğin RSA: Rivest Shamir Adleman) ve simetrik şifreleme (Örneğin AES: Advanced Encryption Standard), bulut bilişim ortamında yaygın olarak kullanılan yöntemlerdir. Simetrik şifreleme, hızlı ve verimli olması nedeniyle büyük veri kümeleri için tercih edilirken, asimetrik şifreleme genellikle kimlik doğrulama ve anahtar yönetimi gibi süreçlerde kullanılır. Ancak, şifreleme yalnız başına veri gizliliğini tam anlamıyla sağlayamaz. Şifreleme anahtarlarının güvenli bir şekilde yönetilmesi ve saklanması, bu sürecin en hassas noktalarından biridir. Anahtarların kaybedilmesi veya çalınması durumunda, şifrelenmiş verilerin erişilemez hale gelmesi gibi ciddi sorunlar ortaya çıkabilir (Barona ve Anita, 2017).

Bunun yanı sıra, homomorfik şifreleme (FHE: Fully Homomorphic Encryption) gibi ileri düzey teknolojiler, verilerin şifresini çözmeden işlenmesine imkân tanıyarak hem gizliliği hem de işlevselliği artırmayı hedeflemektedir. Ancak, bu tür yöntemlerin henüz geniş çapta uygulanabilir olmaması, bulut kullanıcıları için bir sınırlama oluşturmaktadır. Ayrıca, kullanıcıların ve sağlayıcıların veri gizliliğini sağlamak için uluslararası düzenlemelere, örneğin GDPR (General Data Protection Regulation) veya KVKK (Kişisel Verilerin Korunması Kanunu) gibi yasal çerçevelere uyum sağlaması gerekmektedir.

Bulut bilişim ortamında şifreleme, veri gizliliğini ve güvenliğini sağlamak için temel bir mekanizma olarak kabul edilmektedir. Şifreleme algoritmaları, verilerin yalnızca yetkili kişiler tarafından erişilebilir olmasını sağlayarak hassas bilgileri yetkisiz erişimlerden korur. AES, DES (Data Encryption Standard) ve Blowfish gibi şifreleme algoritmaları, bulut bilişimde yaygın olarak kullanılan yöntemler arasındadır. Özellikle, AES algoritması, yüksek güvenlik seviyesi ve verimli performansı sayesinde birçok bulut bilişim uygulamasında tercih edilmektedir. Şifreleme algoritmalarının etkinliği, kullanılan anahtar boyutuna ve algoritmanın karmaşıklığına bağlıdır. Büyük anahtar boyutları, kaba kuvvet saldırılarına karşı daha dirençli bir yapı sunar ve verilerin daha güvenli bir şekilde korunmasını sağlar (Shukla vd., 2021).

Bununla birlikte, şifreleme yalnızca veri koruma sürecinin bir parçasıdır. Şifreleme anahtarlarının güvenli bir şekilde yönetilmesi ve saklanması, veri gizliliğini sağlamada kritik bir rol oynar. Anahtar yönetiminde meydana gelen eksiklikler, şifrelenmiş verilerin yetkisiz kişiler tarafından ele geçirilmesine neden olabilir. Ayrıca, veri iletim sürecinde şifreleme algoritmalarının doğru bir şekilde uygulanmaması, bilgilerin siber saldırılara açık hale gelmesine yol açabilir. Modern bulut bilişim ortamlarında kullanılan şifreleme tekniklerinin, veri gizliliği ile performans arasında bir denge sağlaması gerekmektedir.

Sonuç olarak, şifreleme teknolojileri, bulut bilişimde veri gizliliğinin korunması için güçlü bir savunma hattı sağlarken, bu teknolojilerin doğru bir şekilde uygulanması ve sürekli güncellenmesi, veri güvenliği stratejilerinin başarısı için hayati öneme sahiptir.

3.3.5. Mevzuata Uyumluluk ve Veri Yönetişimi

Bulut bilişimde, Genel Veri Koruma Yönetmeliği (GDPR) gibi düzenlemelere uyumluluk, veri işleme süreçlerinin şeffaflığı ve hesap verilebilirliği açısından kritik bir gerekliliktir. GDPR, Avrupa Birliği tarafından 25 Mayıs 2018'de yürürlüğe giren, bireylerin kişisel verilerinin korunmasını amaçlayan bir düzenlemedir. Bu yönetmelik, kişisel verilerin toplanması, işlenmesi, saklanması ve paylaşılması süreçlerini düzenlerken, bireylerin mahremiyet haklarını güçlendirmeyi hedefler. GDPR'nin hesap verebilirlik ilkesi, bulut sağlayıcıların veri işleme faaliyetlerini kaydetmelerini ve bu faaliyetlerin düzenlemelere uygun olduğunu kanıtlamalarını zorunlu kılar. Bununla birlikte, büyük ölçekli veri akışlarının olduğu bulut ortamlarında, bu tür bir uyumluluğu sağlamak teknik zorluklar meydana getirir. Özellikle, verilerin değiştirilemez bir şekilde kaydedilmesi ve bu kayıtların şeffaf bir biçimde denetlenebilmesi, kullanıcı güvenini artıran temel unsurlardır (Zhou vd., 2023).

Bu tür gereksinimleri karşılamak için blockchain (Blok Zinciri) tabanlı sistemler yaygın olarak kullanılmaktadır. Blockchain, işlem geçmişinin değiştirilemezliğini sağlamak ve kullanıcılar için güven oluşturmak amacıyla sıkça tercih edilmektedir. Ancak, bu yaklaşımlar, blockchain teknolojisinin işlem kapasitesi sınırlamaları ve yüksek maliyetleri nedeniyle pratikte bazı zorluklarla karşılaşmaktadır. Alternatif çözümler arasında, güvenilir yürütme ortamları ve şeffaf veri saklama sistemleri kullanılarak veri bütünlüğünün ve uyumluluğun sağlanması önerilmektedir. Ayrıca, bu çözümler, GDPR uyumluluğunu desteklemek için olay kayıtlarının tutulması ve bu kayıtların denetlenebilir bir yapıda sunulması gibi gereksinimleri karşılayabilir.

Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK-24 Mart 2016), veri işleme süreçlerine ilişkin yasal çerçeve oluşturarak, kişisel verilerin korunması ve veri yönetişimi konularında önemli yükümlülükler getirmiştir. KVKK, veri sorumlularının kişisel verileri hukuka uygun şekilde işlemesini, güvenliğini sağlamasını ve bireylerin veri üzerindeki haklarını korumasını zorunlu kılar. Kanun, verilerin yalnızca belirli, açık ve meşru amaçlarla işlenmesini ve işlenme amacının sona ermesi durumunda imha edilmesini şart koşar. Ayrıca, veri sorumluları için bir Veri Sorumluları Sicil Bilgi Sistemi oluşturulmuş, bu sistem aracılığıyla verilerin şeffaf bir şekilde yönetilmesi hedeflenmiştir. Veri yönetişimi kapsamında, veri sorumlularının düzenli denetim mekanizmaları kurması ve verilerin gizliliğini sağlayacak teknik ve idari tedbirler alması gereklidir. KVKK'ya uyum sağlanmadığı durumlarda, yalnızca idari para cezalarıyla karşılaşılmakla kalınmaz, aynı zamanda bireylerin mahremiyet haklarının ihlali nedeniyle itibar kaybı gibi risklerle de karşılaşılabilir. Bu bağlamda, KVKK, yalnızca yasal uyumluluğu değil, aynı zamanda kişisel verilerin doğru ve etkin bir şekilde yönetilmesini teşvik eden bir araç olarak değerlendirilmektedir (Kişisel Verileri Koruma Kurumu, 2024).

Sonuç olarak, mevzuata uyumluluk ve veri yönetişimi, yalnızca yasal gereklilikleri yerine getirmekle kalmayıp, aynı zamanda bulut sağlayıcılarının kullanıcı güvenini artırmasına da yardımcı olan bir stratejik avantaj sağlamaktadır.

3.4. Bulut Bilişimde Güvenlik Yaklaşımları

Bulut bilişim teknolojilerinin hızla benimsenmesi, beraberinde veri güvenliği ve mahremiyetle ilgili çeşitli sorunları gündeme getirmiştir. Bu bağlamda, güvenlik yaklaşımları, bulut tabanlı sistemlerin korunmasında kritik bir rol oynamaktadır. Güvenlik yaklaşımları, yalnızca verilerin bütünlüğünü ve gizliliğini sağlamakla kalmaz, aynı zamanda kullanıcıların bu teknolojilere olan güvenini artırarak bulut bilişim ekosisteminin sürdürülebilirliğine katkıda bulunur (Zissis ve Lekkas, 2012).

Günümüzde, bulut bilişimde kullanılan güvenlik yaklaşımları, şifreleme tekniklerinden yapay zekâ tabanlı tehdit tespit sistemlerine kadar geniş bir yelpazede çeşitlenmiştir. Bu yaklaşımlar, kullanıcı verilerinin yetkisiz erişimlere karşı korunmasını ve veri kayıplarının önlenmesini hedeflemektedir. Özellikle, "Zero Trust Architecture" (Sıfır Güven Mimarisi) gibi modern yaklaşımlar, veri güvenliğini kapsamlı bir şekilde ele almayı amaçlamaktadır (Kindervag, 2010). Bununla birlikte, bu yaklaşımların etkinliği, kullanılan teknolojinin karmaşıklığına ve bulut sağlayıcılarının uygulama kapasitesine bağlıdır (Hashizume vd., 2013).

Zero Trust Architecture (ZTA), modern siber güvenlik yaklaşımları arasında öne çıkan bir model olup, "asla güvenme, her zaman doğrula" prensibine dayanır. Bu mimaride, ağ içerisindeki veya dışarısındaki hiçbir kullanıcıya veya cihaza otomatik olarak güvenilmez; her erişim talebi, kullanıcının kimliği, bağlamsal faktörler ve cihazın güvenlik durumu gibi kriterlere göre doğrulanır (Kindervag, 2010). Özellikle bulut bilişim ortamında, ZTA, geleneksel güvenlik yöntemlerinin ötesine geçerek daha dinamik ve kapsamlı bir koruma sağlar. Bu yaklaşım, çok faktörlü kimlik doğrulama (MFA), dinamik erişim

kontrolü ve sürekli izleme gibi teknolojilerle desteklenerek, veri sızıntılarını ve yetkisiz erişimleri en aza indirmeyi amaçlar. Zero Trust, bulut bilişimde veri güvenliği sağlayan etkili bir strateji olarak, kullanıcıların ve cihazların kimliklerini sürekli olarak doğrulayarak güvenlik açıklarını azaltır ve organizasyonların dijital varlıklarını daha güvenli bir şekilde korumasına olanak tanır.

Bu bölümde, bulut bilişimde kullanılan güvenlik yaklaşımları detaylı bir şekilde ele alınacak, bu yaklaşımların avantajları ve sınırlamaları tartışılacaktır. Ayrıca, gelecekte veri güvenliğini artırmaya yönelik yenilikçi yaklaşımlar ve teknolojik eğilimler değerlendirilecektir. Bu değerlendirmeler, bulut bilişim kullanıcıları ve sağlayıcıları için hem teorik hem de pratik bir rehber sunmayı amaçlamaktadır.

3.4.1. Şifreleme Teknikleri

Bulut bilişimde veri güvenliğini sağlamak için kullanılan şifreleme teknikleri, hassas bilgilerin korunmasında kritik bir rol oynamaktadır. Şifreleme, verilerin yalnızca yetkili kullanıcılar tarafından okunabilir olmasını sağlayan matematiksel algoritmalarla gerçekleştirilir ve hem veri depolama hem de veri aktarımı sırasında güvenlik sağlar (Barona ve Anita, 2017). Özellikle simetrik ve asimetrik şifreleme yöntemleri, bulut bilişimde yaygın olarak kullanılmaktadır.

Simetrik Şifreleme: Simetrik şifreleme, aynı anahtarın hem şifreleme hem de şifre çözme işlemlerinde kullanıldığı bir yöntemdir. Bu yöntem, hız ve işlem verimliliği açısından avantajlıdır ve büyük veri kümeleri için ideal bir seçenek olarak öne çıkar. Advanced Encryption Standard (AES) gibi algoritmalar, simetrik şifrelemenin popüler bir örneğidir. AES hem güvenilirliği hem de performansı nedeniyle birçok bulut tabanlı uygulamada tercih edilmektedir (Shukla vd., 2021).

Asimetrik Şifreleme: Asimetrik şifreleme, iki farklı anahtarın (Bir açık anahtar ve bir özel anahtar) kullanıldığı bir yöntemdir. Bu yaklaşım, özellikle kimlik doğrulama ve dijital imza süreçlerinde etkilidir. Rivest–Shamir–Adleman (RSA) algoritması, asimetrik şifrelemenin en bilinen örneklerinden biridir. Ancak, işlem yoğunluğu nedeniyle büyük veri kümeleri yerine daha küçük veri setlerinde kullanımı tercih edilmektedir (Zhang vd., 2010).

Homomorfik Şifreleme: Son yıllarda, homomorfik şifreleme gibi yenilikçi yöntemler, veri gizliliğini sağlarken aynı zamanda verilerin şifresi çözülmeden işlenmesine olanak tanıyarak dikkat çekmektedir. Homomorfik şifreleme, özellikle hassas verilerin üçüncü taraflar tarafından işlenmesi gereken durumlarda büyük bir avantaj sağlar. Ancak, bu yöntemlerin yüksek işlem maliyeti ve karmaşıklığı, geniş çaplı uygulamalarını sınırlamaktadır (Gentry, 2009).

Şifreleme Anahtarlarının Yönetimi: Şifreleme anahtarlarının güvenli bir şekilde saklanması ve yönetilmesi, şifreleme sistemlerinin etkinliği için kritik bir öneme sahiptir. Anahtarların kaybedilmesi veya çalınması, şifrelenmiş verilerin erişilemez hale gelmesine yol açabilir. Bu nedenle, anahtar yönetim sistemlerinin güvenli ve kullanıcı dostu bir şekilde tasarlanması gerekmektedir (Barona ve Anita, 2017).

Bulut bilişimde kullanılan şifreleme teknikleri, veri güvenliğini artırmada etkili bir araç sunarken, bu tekniklerin doğru bir şekilde uygulanması ve yönetilmesi hayati öneme sahiptir. Gelecekte, kuantum şifreleme gibi yenilikçi yaklaşımların, bulut bilişimde güvenliği daha da artırması beklenmektedir.

3.4.2. Kimlik ve Erişim Yönetimi (IAM)

Kimlik ve Erişim Yönetimi (IAM: Identity and Access Management), bulut bilişimde güvenliğin temel taşlarından birini oluşturmaktadır. IAM, yalnızca yetkili kullanıcıların belirli kaynaklara erişmesini sağlayarak, veri güvenliğini artırmayı hedefleyen bir çerçevedir (Kanagasabapathi vd., 2016). Bu sistemler, kullanıcı kimlik doğrulama ve yetkilendirme süreçlerini organize ederken, aynı zamanda erişim politikalarını merkezi bir yapı ile yönetmeyi mümkün kılar.

IAM'in Temel Bileşenleri;

- Kimlik Doğrulama (Authentication): Kullanıcıların kimliğinin doğrulanmasını sağlayan süreçtir. Geleneksel yöntemler şifre tabanlı olsa da, modern IAM sistemlerinde çok faktörlü kimlik doğrulama (MFA) yaygın olarak kullanılmaktadır. MFA, şifrelerin yanı sıra biyometrik doğrulama veya fiziksel cihazların kullanımıyla güvenliği artırır (Aloul vd., 2009).
- Erişim Kontrolü (Access Control): Kullanıcıların yalnızca yetkilendirildikleri verilere ve kaynaklara erişebilmesini sağlar. Role-Based Access Control (RBAC) gibi modeller, erişim haklarının kullanıcı rolleri üzerinden yönetilmesine olanak tanır (Kindervag, 2010).

- Politika Yönetimi (Policy Management): IAM çözümleri, erişim politikalarının tanımlanması ve uygulanması için güçlü araçlar sunar. Örneğin, "Zero Trust" yaklaşımı, tüm kullanıcıların sürekli olarak doğrulanmasını gerektirir ve erişim haklarını dinamik olarak değerlendirir.

Bulut bilişim ortamlarında verilerin farklı lokasyonlarda depolanması ve işlenmesi, IAM çözümlerini daha kritik hale getirmektedir. Özellikle, paylaşılan bulut altyapılarında kimlik doğrulama eksiklikleri, veri güvenliği açıklarına neden olabilir. IAM sistemleri, bu riskleri minimize etmek için kullanıcıların ve cihazların güvenliğini bir bütün olarak ele alır (Subashini ve Kavitha, 2011).

Modern IAM Yaklaşımları;

- Biometrik Kimlik Doğrulama: Parmak izi, yüz tanıma veya iris taraması gibi yöntemlerle kullanıcının fiziksel özellikleri üzerinden doğrulama yapılmasını sağlar.
- Blockchain Tabanlı IAM: Merkezi olmayan yapısı sayesinde, kullanıcı kimlik bilgilerinin daha güvenli bir şekilde saklanmasını ve doğrulanmasını mümkün kılar (Zhou vd., 2023).
- Dinamik Erişim Kontrolü: Kullanıcıların davranışlarını analiz ederek erişim izinlerini gerçek zamanlı olarak düzenler. Bu yaklaşım, yapay zekâ tabanlı tehdit tespit sistemleriyle bütünleşmiş olarak çalışabilir.

IAM sistemlerinin uygulanması sırasında, özellikle kimlik doğrulama süreçlerinin karmaşıklığı ve kullanıcı deneyimini olumsuz etkileme potansiyeli, sık karşılaşılan sorunlar arasındadır. Bu zorlukların aşılabilmesi için kullanıcı dostu arayüzler ve esnek yönetim araçları geliştirilmelidir. Ayrıca, IAM sistemlerinin düzenli olarak güncellenmesi ve yeni tehditlere karşı dayanıklılığının artırılması gerekmektedir (Gonzalez vd., 2012).

Kimlik ve erişim yönetimi, bulut bilişim güvenliğinde kritik bir rol oynar. IAM çözümleri hem bireysel kullanıcılar hem de kurumsal işletmeler için, verilerin gizliliğini ve bütünlüğünü sağlamada temel bir savunma mekanizması sunmaktadır.

3.4.3. Güvenlik Duvarları ve İzleme Sistemleri

Bulut bilişimde güvenlik duvarları ve izleme sistemleri, veri güvenliğini sağlamak ve siber tehditlere karşı korunmak için kritik bir öneme sahiptir. Güvenlik duvarları, bir sistem ile dış ortam arasındaki trafiği kontrol ederek yetkisiz erişimleri engellerken, izleme sistemleri, anormallikleri ve potansiyel saldırıları gerçek zamanlı olarak tespit etmek için tasarlanmıştır (Rittinghouse ve Ransome, 2010).

Güvenlik Duvarları: Güvenlik duvarları, bulut ortamındaki veri trafiğini filtreleyerek zararlı girişimleri önler. Geleneksel güvenlik duvarları, IP adresi, protokol ve port numarası gibi parametrelere dayalı olarak trafiği yönetirken, modern güvenlik duvarları (Örneğin Uygulama Katmanı Güvenlik Duvarları) daha gelişmiş özellikler sunar. Bu duvarlar, verilerin içeriklerini analiz ederek kötü niyetli kodları ve anormallikleri tespit edebilir (Gonzalez vd., 2012).

Güvenlik duvarlarını genel yapısı itibari ile ikiye ayırabiliriz. Statik güvenlik duvarları ve dinamik güvenlik duvarları. Statik güvenlik duvarları, trafiği belirli kurallara göre filtreleyen temel sistemlerdir. Ancak, dinamik tehditler karşısında sınırlı bir koruma sağlarlar. Dinamik güvenlik duvarları ise trafiği analiz ederek gerçek zamanlı tehditlere karşı cevap verir ve kullanıcı davranışlarına göre adaptasyon gösterir.

İzleme Sistemleri: İzleme sistemleri, bulut ortamındaki güvenlik ihlallerini tespit etmek ve önlemek amacıyla ağ ve sistem trafiğini sürekli olarak gözlemler. Bu sistemler, genellikle aşağıdaki iki yaklaşımı kullanır:

- Anomali Tabanlı İzleme: Normal trafik desenlerini öğrenir ve bu desenlerden sapmaları tespit eder. Bu yöntem, sıfırıncı gün (Zero-day: Sıfır Gün Saldırıları, henüz keşfedilmiş ancak düzeltilmemiş güvenlik açıklarını hedef alan, sistemlerin savunmasız olduğu kritik saldırılardır.) saldırıları gibi bilinmeyen tehditlere karşı etkilidir (Zissis ve Lekkas, 2012).
- İmza Tabanlı İzleme: Daha önce tanımlanmış tehditlerin imzalarını karşılaştırarak potansiyel saldırıları tespit eder. Bu yöntem, bilinen tehditler için yüksek başarı oranına sahiptir ancak yeni tehditler karşısında etkisiz kalabilir (Hashizume vd., 2013).

Modern Güvenlik Duvarı ve İzleme Çözümlerini şu şekilde sınıflandırabiliriz;

- Yapay Zekâ Tabanlı Sistemler: Yapay zekâ ve makine öğrenimi algoritmaları kullanılarak hem güvenlik duvarlarının hem de izleme sistemlerinin etkinliği artırılmaktadır. Bu sistemler, tehditlerin tahmin edilmesi ve engellenmesinde proaktif bir yaklaşım sunar.
- SIEM (Security Information and Event Management): Güvenlik olaylarını ve tehditlerini merkezi bir şekilde analiz eden ve raporlayan sistemlerdir. SIEM, log analizi yaparak güvenlik açıklarını tespit eder ve bu açıkların giderilmesi için çözüm yolları önerir (Kindervag, 2010).

Güvenlik duvarları ve izleme sistemlerinin uygulanmasında karşılaşılan başlıca zorluklar arasında, performans sorunları, yanlış pozitif alarmlar ve kaynak kullanımındaki verimsizlikler yer almaktadır. Performans sorunları, özellikle yüksek trafiğe sahip büyük ölçekli bulut altyapılarında dikkat çeker. Güvenlik duvarlarının ve izleme sistemlerinin trafiği gerçek zamanlı olarak analiz etme gerekliliği, sistem kaynaklarını yoğun bir şekilde tüketebilir ve bu durum, hizmetlerin performansını olumsuz etkileyebilir (Zhang vd., 2010).

Yanlış pozitif alarmlar, güvenlik sistemlerinin hassasiyetini artırırken, meşru aktivitelerin saldırı olarak algılanmasına neden olabilir. Bu durum, güvenlik ekiplerinin gereksiz müdahalelerde bulunmasına yol açarak zaman kaybına ve kaynak israfına neden olur. Yanlış pozitiflerin en aza indirilebilmesi için güvenlik sistemlerinin sürekli olarak optimize edilmesi ve tehdit algılama algoritmalarının daha hassas hale getirilmesi gerekmektedir (Subashini ve Kavitha, 2011).

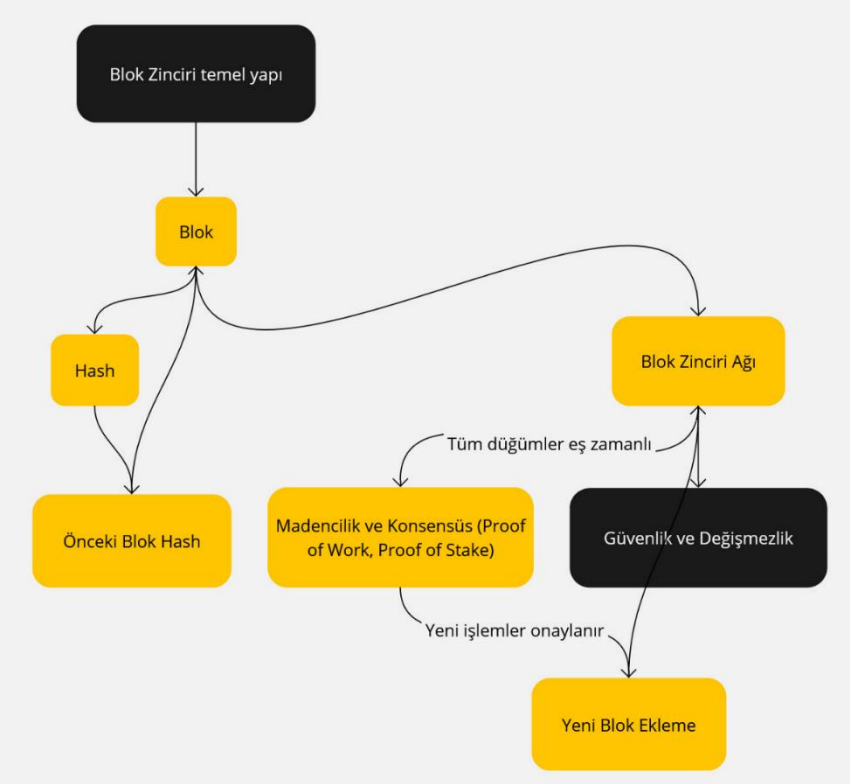
Bu zorlukların üstesinden gelmek için birkaç yenilikçi çözüm önerilmektedir:

- Dağıtık İzleme Sistemleri: Büyük ölçekli bulut altyapılarında, merkezi sistemlerin yerine dağıtık izleme sistemlerinin kullanılması önerilmektedir. Bu sistemler, veri trafiğini yerel seviyede analiz ederek merkezi yükü azaltır ve performansı artırır.
- Otomatik Öğrenme Mekanizmaları: Makine öğrenimi algoritmaları, tehdit algılama sistemlerinin daha akıllı ve etkili çalışmasını sağlar. Bu mekanizmalar, zamanla yeni tehditleri öğrenerek kendini optimize eder ve yanlış pozitiflerin oranını azaltır.
- Yapay Zekâ Destekli Güvenlik Çözümleri: Yapay zekâ tabanlı çözümler, anormallik tespitinde ve tehditlerin sınıflandırılmasında yüksek doğruluk oranları sunar. Bu yaklaşımlar, sistemlerin daha öngörülebilir hale gelmesine ve proaktif güvenlik önlemlerinin uygulanmasına olanak tanır (Hashizume vd., 2013).

Sonuç olarak, güvenlik duvarları ve izleme sistemleri, bulut bilişimde veri güvenliğini artırmak için vazgeçilmez araçlar olarak öne çıkmaktadır. Ancak, bu araçların modern teknolojilerle entegre edilmesi ve sürekli güncellenmesi, etkinliklerinin artırılması açısından hayati önem taşır. Gelecekte, bu sistemlerin yapay zekâ ve Blockchain gibi yenilikçi teknolojilerle güçlendirilmesi, bulut kullanıcılarının karşılaştığı tehditlere karşı daha güçlü bir savunma hattı oluşturacaktır (Gonzalez vd., 2012).

3.4.4. Blockchain Teknolojisinin Kullanımı

Blockchain teknolojisi, bulut bilişim ortamında veri güvenliğini artırmak ve güvenli veri yönetimi sağlamak için yenilikçi bir çözüm sunmaktadır. Merkeziyetsizlik, blockchain'in en önemli özelliklerinden biri olup, verilerin tek bir otoriteye bağlı olmadan yönetilmesini sağlar. Bu özellik, verilerin kontrolünü kullanıcıların eline geçirerek, veri manipülasyonu ve yetkisiz erişim risklerini önemli ölçüde azaltır. Ayrıca, değiştirilemezlik ilkesi sayesinde, blockchain üzerinde kaydedilen veriler geri alınamaz ve değiştirilmesi mümkün değildir. Bu, veri bütünlüğünü sağlamada kritik bir avantaj sunar ve veri kayıpları veya siber saldırılar karşısında güvenilir bir çözüm olarak öne çıkar (Dorsala vd., 2021).



Şekil 2. Blok Zincirinin Çalışma Prensibi (Kaynak: Yazar)

Blockchain'in şeffaflık özelliği, tüm işlemlerin izlenebilirliğini artırarak kullanıcı güvenini pekiştirir. Her işlem, değiştirilemez bir kayıt olarak zincire eklenir ve bu da şeffaf bir denetim mekanizması sağlar. Bulut bilişimde, bu özellikler hem bireysel hem de kurumsal kullanıcılar için veri güvenliğini artırırken, aynı zamanda düzenleyici uyumluluk süreçlerini de destekler. Özellikle hassas verilerin işlendiği sektörlerde, blockchain teknolojisi hem güvenlik hem de operasyonel verimlilik açısından bir standart haline gelmektedir.

Ek olarak, blockchain'in akıllı sözleşme yetenekleri, bulut bilişimde veri paylaşımı ve erişim kontrolü gibi kritik süreçleri otomatikleştirme imkânı sunar. Bu sözleşmeler, belirlenen koşullar yerine getirildiğinde otomatik olarak çalışır ve üçüncü taraflara duyulan güven ihtiyacını ortadan kaldırır. Bu, özellikle veri paylaşımı sırasında güvenlik ihlallerini önlemeye yardımcı olur ve veri yönetimi süreçlerini kolaylaştırır (Dorsala vd., 2021).

Blockchain'in yenilikçi yapısı, yalnızca veri güvenliğini artırmakla kalmaz, aynı zamanda bulut bilişim ortamlarında kullanıcıların bu teknolojilere olan güvenini artırarak genel kabul oranını yükseltir. Bu nedenle, blockchain'in bulut bilişimle entegrasyonu, modern veri yönetiminde önemli bir paradigma değişimini temsil etmektedir.

Blockchain'in Bulut Bilişimdeki Uygulamaları;

- Veri Bütünlüğü ve Güvenliği: Blockchain, verilerin değiştirilemez bir şekilde saklanmasını sağlayarak bulut ortamında veri bütünlüğünü garanti eder. Şifreleme ve dijital imza mekanizmaları ile entegre edildiğinde, hassas verilerin yalnızca yetkili taraflarca erişilebilir olmasını sağlar.
- Dağıtık Veri Yönetimi: Blockchain, merkezi bir yöneticiye ihtiyaç duymadan, bulut sağlayıcıları ve kullanıcılar arasında güvenilir bir veri paylaşımı ve yönetim platformu oluşturur. Bu, kullanıcıların veri üzerindeki kontrolünü artırır ve veri manipülasyonunu engeller.
- Akıllı Sözleşmeler: Blockchain tabanlı akıllı sözleşmeler, veri paylaşımı ve kaynak yönetimi süreçlerini otomatikleştirerek, bu işlemlerin şeffaf ve güvenilir bir şekilde yürütülmesini sağlar. Özellikle erişim kontrolü ve veri paylaşımı gibi kritik süreçlerde bu sözleşmeler büyük bir avantaj sunar.
- Güvenli Veri İzlenebilirliği: Blockchain, tüm işlemleri şeffaf bir şekilde kaydederek veri ihlallerinin ve manipülasyonların kaynağını izlemeyi kolaylaştırır. Bu özellik, düzenleyici uyumluluğu sağlamak için kullanılabilir.

Blockchain, veri güvenliği ve şeffaflık konularında önemli avantajlar sunsa da, bazı sınırlamalar da içermektedir.

- Performans Sorunları: Blockchain ağları, yoğun işlem hacmi durumlarında performans düşüşü yaşayabilir.
- Enerji Tüketimi: Özellikle Proof-of-Work (PoW, blockchain ağına yeni bir blok eklemek için kullanılan bir yöntemdir.) gibi mutabakat mekanizmaları, yüksek enerji tüketimine neden olabilir (Tschorsch ve Scheuermann, 2016).
- Uyumluluk ve Entegrasyon: Mevcut bulut altyapıları ile blockchain teknolojisinin entegrasyonu, teknik ve operasyonel zorluklar meydana getirebilir.

3.5. Güncel Araştırmalar ve Çözüm Önerileri

Bulut bilişim ve veri güvenliği alanında yapılan güncel çalışmalar, bu teknolojilerin sunduğu fırsatlar ve karşılaşılan zorluklara yönelik yenilikçi çözümleri detaylı bir şekilde ortaya koymaktadır. Bulut bilişim, büyük veri analitiği, yapay zekâ ve nesnelerin interneti gibi modern teknolojilere entegrasyonu sayesinde işletmelere operasyonel verimlilik, maliyet avantajı ve esneklik sunmaktadır. Ancak, bu avantajlarla birlikte, veri ihlalleri, kimlik doğrulama açıkları ve erişim kontrolü gibi güvenlik risklerini de beraberinde getirmektedir.

Hem akademik araştırmalar hem de sektörel uygulamalar, bu zorlukları aşmak ve bulut bilişim ortamındaki veri güvenliğini artırmak için farklı yaklaşımlar geliştirmiştir. Örneğin, akademik çalışmalar, blockchain teknolojisi gibi yenilikçi çözümlerin veri güvenliğini artırmada önemli bir potansiyele sahip olduğunu göstermektedir. Blockchain'in merkezi olmayan yapısı ve değiştirilemezlik özelliği, veri manipülasyonuna karşı güçlü bir savunma mekanizması sunmaktadır (Dorsala vd., 2021). Bunun yanı sıra, şifreleme algoritmaları ve çok faktörlü kimlik doğrulama (MFA) gibi yöntemler, güvenlik risklerini minimize etmek için etkili araçlar olarak öne çıkmaktadır (Kanagasabapathi, 2016).

Sektörel uygulamalarda ise, özellikle dinamik erişim kontrolü, yapay zekâ tabanlı tehdit analizi ve güvenlik duvarlarının optimize edilmesi gibi yöntemlerin kullanımı yaygınlaşmaktadır. Bu teknolojiler, yalnızca mevcut tehditlere karşı koruma sağlamakla kalmaz, aynı zamanda gelecekteki olası tehditlere karşı proaktif bir savunma mekanizması oluşturur. Özellikle, bulut hizmet sağlayıcılarının sunduğu güvenlik çözümleri, sektörde güvenilirliği artırarak kullanıcıların bu teknolojilere olan güvenini pekiştirmektedir (Dai vd., 2019).

Literatürde Yer Alan Önemli Çalışmalar ve Bulgular;

- Şifreleme ve Veri Bütünlüğü:

  Armbrust ve arkadaşlarının (2010) çalışmasında, bulut bilişimde veri şifrelemenin veri bütünlüğü ve gizliliğini sağlama konusundaki kritik rolü vurgulanmaktadır. AES gibi simetrik şifreleme algoritmalarının, yüksek güvenlik standartları ve performans avantajları nedeniyle tercih edildiği belirtilmiştir (Armbrust, 2010).

  Zhang ve arkadaşlarının (2010) çalışması, bulut bilişimde veri güvenliğiyle ilgili temel sorunları ve mevcut çözümleri kapsamlı bir şekilde ele almaktadır. Şifreleme teknolojilerinin veri bütünlüğünü sağlama konusundaki rolüne vurgu yapılmış ve simetrik şifreleme algoritmaları (örneğin, AES) ile asimetrik algoritmaların (örneğin, RSA) avantajları ve sınırlamaları tartışılmıştır. Çalışmada, özellikle verilerin şifrelenerek depolanması ve taşınması sırasında güvenliğin sağlanması için hibrit şifreleme yöntemlerinin kullanılabileceği önerilmiştir. Bu yaklaşım hem performans hem de güvenlik açısından denge sağlamaktadır (Zhang vd., 2010).

- Kimlik ve Erişim Yönetimi (IAM):

  Kanagasabapathi ve arkadaşlarının (2016) çalışması, kimlik doğrulama ve erişim kontrol sistemlerinin, özellikle paylaşılan bulut altyapılarında veri güvenliğini sağlamada önemli olduğunu göstermektedir. Çok faktörlü kimlik doğrulama (MFA) ve rol tabanlı erişim kontrolü (RBAC) gibi yöntemlerin etkinliği vurgulanmıştır (Kanagasabapathi, 2016).

  Aloul ve arkadaşlarının (2009) çalışması, iki faktörlü kimlik doğrulama (2FA) yönteminin, bulut tabanlı sistemlerde kimlik ve erişim yönetimini güvenli hale getirme konusundaki önemini ele alır. Çalışmada, mobil cihazların bir doğrulama aracı olarak kullanımının, kimlik doğrulama süreçlerinde ek bir güvenlik katmanı sağladığı belirtilmiştir. Ayrıca, 2FA'nın tek faktörlü

doğrulamaya kıyasla yetkisiz erişimleri önlemede daha etkili olduğu vurgulanmış ve bu yöntemin bulut bilişim altyapılarında uygulanabilirliği tartışılmıştır (Aloul vd., 2009).

- Blockchain Teknolojisinin Güvenlikteki Rolü:

  Dorsala ve arkadaşları (2021), blockchain tabanlı çözümlerin bulut bilişimde veri güvenliğini artırmada nasıl kullanılabileceğini incelemiştir. Akıllı sözleşmeler ve dağıtık defter teknolojilerinin, veri bütünlüğü ve şeffaflık sağlama konusundaki katkıları ele alınmıştır (Dorsala vd., 2021).

  Zheng ve arkadaşlarının (2018) çalışması, blockchain teknolojisinin potansiyel uygulama alanları ve karşılaşılan zorluklarını ele alır. Çalışma, blockchain tabanlı çözümlerin özellikle bulut bilişimde veri bütünlüğünü sağlama, erişim kontrolünü yönetme ve şeffaflık sağlama konularındaki rolünü kapsamlı bir şekilde tartışır. Akıllı sözleşmelerin veri paylaşımı ve erişim yönetimi süreçlerindeki avantajlarına dikkat çekilmiş ve dağıtık defter teknolojisinin, veri güvenliğini artırmada nasıl etkin kullanılabileceği örneklerle açıklanmıştır (Zheng vd., 2018).

- Yapay Zekâ Tabanlı Güvenlik Sistemleri:

  Dai ve arkadaşlarının (2019) çalışması, yapay zekâ ve makine öğrenimi algoritmalarının, anomali tespiti ve tehdit analizi süreçlerinde kullanılmasının etkinliğini ortaya koymuştur (Dai vd., 2019).

  Buczak ve Guven (2016), yapay zekâ ve makine öğrenimi yöntemlerinin siber güvenlikteki uygulamalarını ele alan kapsamlı bir çalışma sunmuştur. Çalışmada, özellikle anomali tespiti ve tehdit analizi için kullanılan denetimli ve denetimsiz öğrenme algoritmalarının etkinliği değerlendirilmiştir. Yazarlar, bu algoritmaların siber saldırıları tespit etmedeki başarı oranlarını, performans kıyaslamaları ve örnek vaka çalışmaları ile desteklemiştir. Ayrıca, makine öğrenimi tabanlı güvenlik sistemlerinin, mevcut güvenlik çözümlerine nasıl entegre edilebileceği ve karşılaşılan zorluklara yönelik çözüm önerileri tartışılmıştır (Buczak vd., 2016).

Bulut bilişimde veri güvenliğini artırmak için geliştirilen yenilikçi çözümler hem akademik çalışmaların teorik çerçevelerinden hem de sektördeki uygulamaların pratik deneyimlerinden beslenmektedir. Akademik araştırmalar, bu alandaki güvenlik sorunlarını daha iyi anlamak ve çözüm yolları geliştirmek için kapsamlı analizler sunarken, sektörel yaklaşımlar, bu çözümleri gerçek dünyada uygulanabilir hale getirmeyi amaçlamaktadır. Bu iki perspektifin birleşimi, bulut bilişim güvenliğinde bütüncül ve etkili yaklaşımlar geliştirilmesine olanak tanır. Aşağıda, akademik ve sektörel düzeyde yapılan önerilere yer verilmiştir. Bu öneriler, bulut bilişimde karşılaşılan güvenlik sorunlarına yönelik yenilikçi stratejileri ve iyi uygulama örneklerini içermektedir.

- Standartlaşma Çalışmaları: Literatürde, bulut bilişim ve veri güvenliği alanında standartların geliştirilmesi gerektiği belirtilmektedir. Özellikle, uluslararası düzenlemelerle uyumlu güvenlik protokollerinin benimsenmesi önerilmektedir (Mell ve Grance, 2011).
- Blockchain ve Yapay Zekâ Entegrasyonu: Blockchain ve yapay zekâ tabanlı sistemlerin bir arada kullanılması, veri güvenliği ve yönetimi süreçlerini optimize edebilir. Örneğin, yapay zekâ, blockchain üzerindeki işlemlerin analiz edilmesi ve şüpheli aktivitelerin belirlenmesi için kullanılabilir.
- Eğitim ve Farkındalık Artırma: Sektörel çalışmalar, veri güvenliği konusunda kullanıcı farkındalığını artırmaya yönelik eğitimlerin önemine vurgu yapmaktadır. Ayrıca, bulut hizmet sağlayıcılarının bu konuda müşterilere rehberlik etmesi gerekmektedir.
- Enerji Verimli Çözümler: Güncel araştırmalar, enerji yoğun mutabakat mekanizmalarının yerine enerji verimliliği yüksek alternatiflerin benimsenmesi gerektiğini vurgulamaktadır. Bu bağlamda Proof-of-Stake gibi mekanizmalar önerilmektedir (Tschorsch ve Scheuermann, 2016).

3.5.1. Blok Zincirinin Bulut Bilişimde Kullanımına İlişkin Sektörel Örnekler

Blok zinciri, bulut bilişimle entegre edilerek farklı sektörlerde veri güvenliği, izlenebilirlik ve operasyonel verimlilik açısından önemli katkılar sunmaktadır. Merkezi olmayan yapısı ve değiştirilemezlik gibi özellikleri sayesinde blok zinciri, veri manipülasyonunu önlerken süreçlerin şeffaflığını artırır. Aşağıda, blok zincirinin bulut bilişimdeki kullanımına ilişkin sektörel örneklere yer verilmiştir.

Eğitim Sektörü: MIT Digital Certificates Project, blockchain üzerinde öğrenci diplomalarını saklar. Blockchain, diplomaların doğrulanabilir ve değiştirilemez bir şekilde depolanmasını sağlar (MIT Digital Certificates, 2024).

Enerji Sektörü: Power Ledger, enerji ticareti için blockchain tabanlı bir platformdur. Blockchain, enerji ticaretinde kullanıcılar arasında doğrudan güvenli işlem yapılmasını sağlar (Power Ledger, 2024).

Finans Sektörü: JPMorgan'ın Quorum Platformu, blockchain tabanlı bir finansal veri yönetim sistemidir. Blockchain, finansal işlemlerin kaydını güvenli ve değiştirilemez bir şekilde tutmak için kullanılır. Bu, sahtekarlığı önler ve işlemlerin şeffaflığını artırır (JpMorgan, 204).

Lojistik Sektörü: Maersk ve IBM'in TradeLens Platformu, blockchain tabanlı bir lojistik platformdur. Blockchain, tedarik zincirindeki tüm işlemlerin izlenebilirliğini sağlar ve bu süreçteki güvenlik açıklarını en aza indirir (TradeLens, 2024).

Sağlık Sektörü: MediBloc gibi blockchain tabanlı projeler, sağlık sektöründe hasta verilerinin güvenli bir şekilde saklanmasını ve paylaşılmasını sağlar. Blockchain, hasta bilgilerinin yetkisiz erişimlere karşı korunmasını sağlamak için kullanılır. Bu, hasta bilgilerinin gizliliğini artırırken, sağlık hizmeti sağlayıcıları arasında güvenli bir şekilde paylaşılmasını mümkün kılar (MediBloc, 2024).

Blok zincirinin farklı sektörlerdeki kullanımı, bu teknolojinin yalnızca veri güvenliğini artırmakla kalmayıp, aynı zamanda süreçlerin şeffaflığını ve verimliliğini artırma potansiyelini de göstermektedir. Ancak, bu uygulamaların yaygınlaşması için teknolojinin maliyetleri, entegrasyon zorlukları ve düzenleyici gereksinimlere uyum sağlama konularında daha fazla çalışma yapılması gerekmektedir. Blok zincirinin bulut bilişimle entegrasyonu, gelecekteki araştırmalar ve uygulamalar için umut vadeden bir alan olarak öne çıkmaktadır.

Sektörel uygulamaların akademik çalışmalarla da uyumlu olduğunu gösteren Hackius ve Petersen'in (2017) çalışması blok zinciri kullanımına dikkati çekmektedir. Bu çalışmaya göre Maersk ve IBM'in TradeLens platformu, blockchain teknolojisini lojistik süreçlerinde etkin bir şekilde kullanarak tedarik zincirindeki işlemleri izlenebilir hale getirmiştir. Bu uygulama, Hackius ve Petersen'in blockchain'in lojistikteki faydalarına yönelik teorik bulgularıyla uyum göstermektedir. Yazarlar, blockchain'in güvenlik açıklarını azaltmada ve şeffaflığı artırmada kritik bir rol oynadığını vurgulamaktadır. TradeLens bu teoriyi pratiğe dökerek, sektör için yenilikçi bir çözüm sunmuştur (Hackius ve Petersen, 2017).

4. SONUÇ

Bulut bilişim teknolojileri, sunduğu esneklik, maliyet avantajı ve ölçeklenebilirlik gibi özelliklerle modern bilgi teknolojilerinin temel taşlarından biri haline gelmiştir. Ancak, bu teknolojinin yaygınlaşması, veri güvenliği ve mahremiyetle ilgili önemli sorunları da beraberinde getirmiştir. Bu çalışmada, bulut bilişimde karşılaşılan veri güvenliği sorunları detaylı bir şekilde ele alınmış ve bu sorunlara yönelik çözüm önerileri literatürden yararlanılarak tartışılmıştır.

Çalışma kapsamında, şifreleme teknikleri, kimlik ve erişim yönetimi, güvenlik duvarları ve blockchain gibi modern güvenlik yaklaşımlarının bulut bilişimdeki etkinliği analiz edilmiştir. Özellikle, blockchain tabanlı çözümler, veri bütünlüğü, şeffaflık ve güvenilirlik sağlama konularında büyük bir potansiyele sahiptir. Bunun yanı sıra, yapay zekâ tabanlı güvenlik sistemleri ve homomorfik şifreleme gibi yenilikçi yöntemler, veri güvenliği alanında gelecekteki araştırmalar için umut vaat etmektedir.

Bulgular, yalnızca teknik çözümler sunmakla kalmayıp, aynı zamanda bulut bilişim kullanıcılarının bilinçlendirilmesi ve sektörde daha etkili düzenleyici politikaların benimsenmesi gerektiğini de göstermektedir. Güçlü kimlik doğrulama yöntemleri ve erişim kontrol politikalarının uygulanması, kullanıcı hatalarından kaynaklanan güvenlik açıklarının azaltılmasında kritik bir rol oynamaktadır. Ayrıca, veri kaybını önlemek için etkili yedekleme stratejilerinin geliştirilmesi ve güvenlik protokollerinin sürekli olarak güncellenmesi gerekmektedir.

Sonuç olarak, bulut bilişimde veri güvenliğinin sağlanması hem teknik hem de organizasyonel düzeyde çok boyutlu bir yaklaşım gerektirmektedir. Teknik düzeyde, şifreleme yöntemlerinin geliştirilmesi, yapay zekâ ve blockchain gibi yenilikçi teknolojilerin entegrasyonu, veri güvenliği sorunlarının çözümünde kritik bir rol oynamaktadır. Özellikle, dinamik tehditlere karşı proaktif bir koruma sağlayan yapay zekâ tabanlı sistemler ve merkezi olmayan veri yönetimi sunan blockchain çözümleri, modern güvenlik stratejilerinin merkezinde yer almaktadır. Organizasyonel düzeyde ise, kullanıcı farkındalığını artırmaya yönelik eğitim

programları ve güvenlik protokollerinin güncel tutulması, insan kaynaklı hataların azaltılması için büyük önem taşımaktadır.

Bu bağlamda, araştırmacılar ve sektör uzmanları arasında daha fazla iş birliği yapılması gereklidir. Akademik çalışmaların teorik çerçevelerinden elde edilen bilgiler ile sektör uygulamalarından gelen pratik deneyimlerin bir araya getirilmesi, daha güçlü ve kapsamlı güvenlik çözümlerinin geliştirilmesine olanak tanıyacaktır. Ayrıca, kamu ve özel sektör iş birlikleri, düzenleyici uyumluluğun sağlanması ve güvenlik standartlarının oluşturulmasında kritik bir rol oynayabilir. Bu iş birliği çabaları hem bireysel kullanıcılar hem de kurumsal işletmeler için bulut bilişim sistemlerini daha güvenli ve kullanıcı dostu hale getirecektir.

Bu çalışma, bulut bilişimde veri güvenliğini sağlamaya yönelik mevcut yöntemler ve gelecekteki araştırma alanları hakkında kapsamlı bir yol haritası sunmayı amaçlamaktadır. Çalışmada ele alınan güvenlik yaklaşımları ve çözüm önerileri, yalnızca günümüz ihtiyaçlarına yanıt vermekle kalmayıp, gelecekte ortaya çıkabilecek tehditlere karşı da sağlam bir temel oluşturmayı hedeflemektedir. Bu bağlamda, enerji verimli mutabakat mekanizmalarından kuantum şifreleme teknolojilerine kadar geniş bir yelpazede yeni araştırma alanları, bulut bilişimde veri güvenliğinin geleceğini şekillendirecektir.

KAYNAKÇA

Aloul, F., Zahidi, S., & El-Hajj, W. (2009, May). Two-factor authentication using mobile phones. In *2009 IEEE/ACS International Conference on Computer Systems and Applications* (pp. 641–644). IEEE.

Amazon Web Services. (2024). What is Amazon VPC? https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

AWS. (2024). *Amazon Web Services*. https://aws.amazon.com

Azure. (2024). *Turn AI curious into AI capable*. https://azure.microsoft.com

Azure Arc. (2024). *Azure Arc*. https://azure.microsoft.com/en-us/products/azure-arc

Azure Stack. (2024). *Azure Stack*. https://azure.microsoft.com/en-us/products/local

Barona, R., & Anita, E. M. (2017). A survey on data breach challenges in cloud computing security: Issues and threats. In *2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT)* (pp. 1–8). IEEE.

Booth, A., Papaioannou, D., & Sutton, A. (2012). *Systematic approaches to a successful literature review.* SAGE Publications.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems, 25*(6), 599–616.

Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, *18*(2), 1153-1176.

California Community Colleges Cloud. (2024, Kasım 19). *Common Cloud Data Platform Demonstration Project*. https://www.cccco.edu/About-Us/Vision-2030/vision-2030-demonstration-projects/common-cloud-data-platform

Carr, N. G. (2008). *The big switch: Rewiring the world, from Edison to Google.* W. W. Norton & Company.

CERN Cloud. (2024). *CERN Cloud*. https://home.cern/science/experiments/cloud

Cloudflare. (2024). *Discover the connectivity cloud.* https://www.cloudflare.com

Cyberwebeyeos. (2024). *Cloudflare, tarihin en büyük DDoS saldırısını önledi.* https://cyberwebeyeos.com/haberler/cloudflare-tarihin-en-buyuk-ddos-saldirisini-onledi

Dai, H., Zheng, Z., Zhang, Y., Chen, S., & Zhang, L. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076–8094.

Dorsala, M. R., Sastry, V. N., & Chapram, S. (2021). Blockchain-based solutions for cloud computing: A survey. *Journal of Network and Computer Applications, 196*, 103246.

Fink, A. (2019). *Conducting research literature reviews: From the internet to paper* (5th ed.). Sage Publications.

Gartner (2023). *Gartner says cloud will become a business necessity by 2028*. Gartner Research. https://www.gartner.com/en/newsroom/press-releases/2023-11-29-gartner-says-cloud-will-become-a-business-necessity-by-2028

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications, 1*(1), 1–18.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178).

GCP. (2024). *Google Cloud Platform*. https://cloud.google.com

Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or treat? In *Proceedings of the Hamburg International Conference of Logistics (HICL)*, (pp. 3-18). https://doi.org/10.15480/882.1444

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernández, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), Article 5. https://doi.org/10.1186/1869-0238-4-5

IBM Security. (2024). *Cost of a data breach report 2024*. IBM. https://www.ibm.com/reports/data-breach

IBM Cloud. (2024). *Hybrid cloud solutions*. IBM. https://www.ibm.com/hybrid-cloud

JpMorgan. (2024). *Next-generation financial infrastructure*. https://www.jpmorgan.com/kinexys/index

Kanagasabapathi, K., Deepak, S., & Prakash, P. (2016). A study on security issues in cloud computing. In L. P. Suresh, B. K. Panigrahi, S. C. Satapathy, & N. K. Kamila (Eds.), *Proceedings of the International Conference on Soft Computing Systems: ICSCS 2015, Volume 2* (pp. 167–175).

Kindervag, J. (2010). *No more chewy centers: Introducing the zero trust model of information security.* Forrester Research.

Kişisel Verileri Koruma Kurumu. (2024). *Kişisel Verilerin Korunması Kanunu.* Kişisel Verileri Koruma Kurumu. https://kvkk.gov.tr

Kitchenham, B. (2004). *Procedures for performing systematic reviews* (Technical Report No. 33). Keele University.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy, 37*(4–5), 372–386. https://doi.org/10.1016/j.telpol.2012.04.011

Marinos, A., & Briscoe, G. (2009). Community cloud computing. In *Proceedings of the First International Conference on Cloud Computing.*

MediBloc. (2024). *Own your health data. It's rightfully yours*. https://medibloc.com

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing.* National Institute of Standards and Technology Special Publication (SP) 800-145. https://doi.org/10.6028/NIST.SP.800-145

MIT Digital Certificates. (2024). *Digital Transformation*. https://professionalprograms.mit.edu/professional-certificate-program-in-digital-transformation

Owasp. (2024). *Comparison between 2016 and 2024*. https://owasp.org/www-project-mobile-top-10

Power Ledger. (2024). *Power Ledger Blockchain*. https://powerledger.io

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009, November). Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (pp. 199–212). ACM.

Rittinghouse, J. W., & Ransome, J. F. (2010). *Cloud computing: Implementation, management, and security*. CRC Press.

Russon, M. (2021). ABD'de siber saldırı: Bilgisayar korsanları ülkenin en büyük boru hattını devre dışı bıraktı, akaryakıt karayoluyla taşınacak. *BBC World*. https://www.bbc.com/turkce/haberler-dunya-57056048

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006

Shukla, D. K., Dwivedi, V. K., & Trivedi, M. C. (2021). Encryption algorithm in cloud computing. *Materials Today: Proceedings*, *37*, 1869–1875.

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, *4*(3), 356–367. https://doi.org/10.1177/1534484305278283

TradeLens. (2024). *Yılport Holding IBM ve Maersk'in blokzinciri platformuna katıldı*. https://bctr.org/yilport-holding-ibm-ve-maerskin-blokzinciri-platformuna-katildi-17874

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084-2123.

VMware. (2024). *What is private cloud?* https://www.vmware.com/topics/private-cloud

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7–18.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375.

Zhou, C., Barati, M., & Shafiq, O. (2023). A compliance-based architecture for supporting GDPR accountability in cloud computing. *Future Generation Computer Systems*, *145*, 104–120.