Journal of Computer Science
https://dergipark.org.tr/en/pub/bbd
Anatolian Science

ISSN,e-ISSN: 2548-1304
Volume:9, Issue: 1 pp:62-71, 20
https://doi.org/ 10.53070/bbd.1448462
Research Paper

Bulut Bilişim Mimarisi ve Güvenliği

Cloud Computing Architecture and Security

Kemal YİGİT [1], Faruk AYATA *[2]

[1]Van Yüzüncü Yıl Üniversitesi, Fen Bilimleri Enstitüsün, Yapay Zekâ ve Robotik ABD, Van, Türkiye

[2]Van Yüzüncü Yıl Üniversitesi, Başkale MYO, Bilgisayar Teknolojileri, Van, Türkiye

(kemal@kemalyigit.com, farukayata@yyu.edu.tr)

Received:Mar.07,2024 Accepted:Apr.16,2024 Published:Jun.01,2024

Özetçe— Bulut bilişim, depolama, işleme, ağ oluşturma ve yazılım gibi çeşitli hizmetlerin internet üzerinden sunulmasını sağlayan sistemlerdir. Bulut bilişim, ölçeklenebilirlik, esneklik, maliyet verimliliği ve erişilebilirlik avantajları nedeniyle son yıllarda büyük ilgi görmektedir. Ancak bulut bilişim aynı zamanda veri ihlalleri, yetkisiz erişim, hizmet reddi ve kötü niyetli saldırılar gibi önemli güvenlik sorunlarını da beraberinde getirmektedir. Bu nedenle bulut hizmetlerinin ve verilerinin güvenliğinin ve gizliliğinin sağlanması hem bulut sağlayıcıları hem de kullanıcılar için çok önemli bir konu haline gelmektedir.

Bu çalışmada, bulut bilişim sistemlerinin temelleri, standartları ve teknoloji enstitülerinin belirlediği kriterleri incelenmektedir. Bulut bilişim mimarisi kapsamında, kullanılan servis modelleri ve dağıtım modelleri üzerinde durulmuştur. Bulut bilişimin faydaları ile birlikte bu alandaki tehdit türleri ve bunlara karşı olası çözümler detaylı bir şekilde ele alınmıştır. Çalışmada, hangi tehditlere karşı hangi çözümlerin etkili olabileceği üzerinde durulmuş ve bu çözümler incelenmiştir. Son olarak, bulut bilişimdeki tehditlere karşı yapay zeka sistemlerinin nasıl kullanılabileceği incelenmiştir. Bu inceleme kriterleri doğrultusunda, bulut bilişim güvenliğinde kapsamlı bir inceleme yapılmaya çalışılmıştır.

Anahtar Kelimeler : *Bulut Bilişim, Yapay Zeka, Bulut Bilişim Güvenliği, Makine Öğrenmesi*

Abstract— Cloud computing is systems that provide various services such as storage, processing, networking and software over the internet. Cloud computing has attracted great attention in recent years due to its scalability, flexibility, cost efficiency and accessibility advantages. However, cloud computing also brings with it significant security problems such as data breaches, unauthorized access, denial of service and malicious attacks. Therefore, ensuring the security and privacy of cloud services and data becomes a very important issue for both cloud providers and users.

This study examines the fundamentals of cloud computing systems, standards, and the criteria set by technology institutes. Within the scope of cloud computing architecture, the focus is on the service models and deployment models used. Alongside the benefits of cloud computing, the types of threats in this field and possible solutions against them are thoroughly discussed. The study emphasizes which solutions could be effective against which threats and examines these solutions. Finally, the potential use of artificial intelligence systems against threats in cloud computing is explored. Following these examination criteria, a comprehensive review of cloud computing security is attempted.

Keywords : *Cloud Computing, Artificial Intelligence, Cloud Computing Security, Machine Learning*

1. Giriş

Bulut bilişim, bilgisayar kaynaklarının (veri depolama, işlem gücü, yazılım gibi) internet üzerinden paylaşıldığı ve istemcilerin ihtiyaçlarına göre hizmetlerin sunulduğu bir bilgi işlem modelidir. Bu modelde kullanıcılar, kendi donanım ve yazılımlarını satın alıp bakımını yapmak yerine, bu hizmetleri bulut hizmet sağlayıcılarından kiralayabilmektedir. Bulut bilişim, kullanıcılara esneklik, ölçeklenebilirlik ve maliyet avantajı kazandırmanın yanı sıra işletmelerin ve bireylerin BT (Bilişim Teknolojileri) altyapılarına erişimini kolaylaştırarak iş sürekliliği, güvenlik, veri yedekleme gibi konulara çözüm sunmaktadır. Verilerin iletilmesi ve saklanması gibi süreçleri kolaylaştıran bulut bilişimin hayatımıza girmesi internetin girişiyle aynı zamana denk gelmiş ve internet kullanıcı sayısının artması bulut bilişime olan ihtiyacın artmasına neden olmuştur.

Yapay zeka (AI), bulut bilişim teknolojileri ile entegre olarak, veri yönetimi, işlem optimizasyonu, güvenlik ve inovasyon alanlarında önemli katkılar sağlamaktadır. Yapay zeka, büyük veri setlerinin otomatik işlenmesi, akıllı veri depolama çözümleri sunarak veri yönetimini iyileştirirken, kaynak tahsisi ve otomasyon ile bulut bilişim kaynaklarının daha etkin kullanımını destekler. Bu entegrasyonla, işletmelerin rekabet avantajı elde etmesine ve teknolojik inovasyonun sınırlarını zorlamasına olanak tanıyarak dijital dönüşüm süreçlerinde kritik bir rol oynamaktadır. Bu kapsamlı etkileşim, yapay zekanın bulut bilişime katkısını, sadece mevcut işlevselliği artırmanın ötesinde, yeni hizmet modellerini mümkün kılan bir dönüşüm olarak öne çıkarır.

Günümüzde buluttaki depolama, işlem gücü ve yazılım sistemleri genişlemeye devam ettikçe, bu büyüme güvenlik sorunlarına yeni boyutlar getirmekte ve veri koruma ve gizliliği sağlamak için bulut bilişimde güvenlik sistemlerinin kullanılmasına yol açmaktadır. Yapay zeka sistemleri analiz ve yorumlama, problem çözme ve muhakeme, örüntü tanıma, analojileri tespit etme, öğrenme, bilgiyi saklama ve alma, karmaşık problemleri çözme, sınıflandırma ve genelleme, yeni durumlara uyum sağlama ve daha birçok alanda üstün yeteneklere sahiptir. Bu yetenekler, bulut bilişim güvenliğindeki önemli rolünü göstermektedir. Bu çalışma, tehditleri tespit etme, siber saldırıları önleme ve güvenlik önlemlerini sürekli güncelleme gibi kritik işlevleri yerine getirebilecek yapay zeka sistemleri ve bulut bilişime ilişkin araştırmaları içermektedir.

Literatür taraması sürecinde, merkezi veritabanlarından seçilen anahtar kelimelerle yapılan aramalar neticesinde elde edilen kaynaklar, yayın tarihlerine göre kronolojik olarak sıralanıp incelenmiştir. Araştırmanın kapsamını genişletmek adına, seçilen makalelerin referansları da indirilerek analize dahil edilmiştir. Tarama stratejisi, özellikle son yıllarda yayımlanan literatür üzerine yoğunlaşmış, ancak bu çalışmaların atıfta bulunduğu daha eski ve konuya dair önemli açıklamalar içeren kaynaklar da göz ardı edilmemiştir. Bu süreçte, yaklaşık 300 kaynak gözden geçirilmiş ve bunlar arasından konu bütünlüğü sağlayan 41 kaynak referans listesine eklenmiştir. çalışmanın devamında literatür taramasına ilişkin beş adet kaynağa ilişkin bilgi yer almaktadır. Çalışma boyunca yer alan kaynaklar, konunun daha geniş bir perspektiften anlaşılmasına katkı sağlamaktadır.

Hasimi ve ark. (2023) “Bulut Bilişim Güvenliği ve Derin Öğrenme: Bir Yapay Sinir Ağı yaklaşımı” isimli çalışma ile derin öğrenme ve yapay sinir ağları gibi modellerin bulut bilişim güvenliği uygulamalarında tehdit algılamanın otomatikleştirilmesi ile manuel izlemenin azaltılması sonucu izinsiz giriş tespiti, kötü amaçlı yazılım tespiti, anormallik tespiti ve günlük analizi gibi görevlerde önemli roller oynayacağını örnek veri seti üzerinden incelemiştir. Örnek veri setinde yapılan test sonuçları ile sistemin pratik olarak iyi olduğu doğrulanmış. Eğitim setinin büyüklüğünün artırılması ile güvenlik tehditlerinin gerçek zamanlı olarak tespit edilebileceği ve risklerin aza indirilebileceğinden bahsedilmiştir.

Zawaideh ve ark (2022) “Bulut Bilişim Altyapısının Katmanları ve Güvenlik Saldırısı Sorunları” isimli çalışma ile internet kullanıcılarının ayrılmaz bir parçası haline gelen bulut bilişimin çeşitli yönleriyle güvenlik sorunları ele alınmış. Sektörel standartlar ile bulut bilişimin güvenliğinin artırılacağı belirtmiştir.

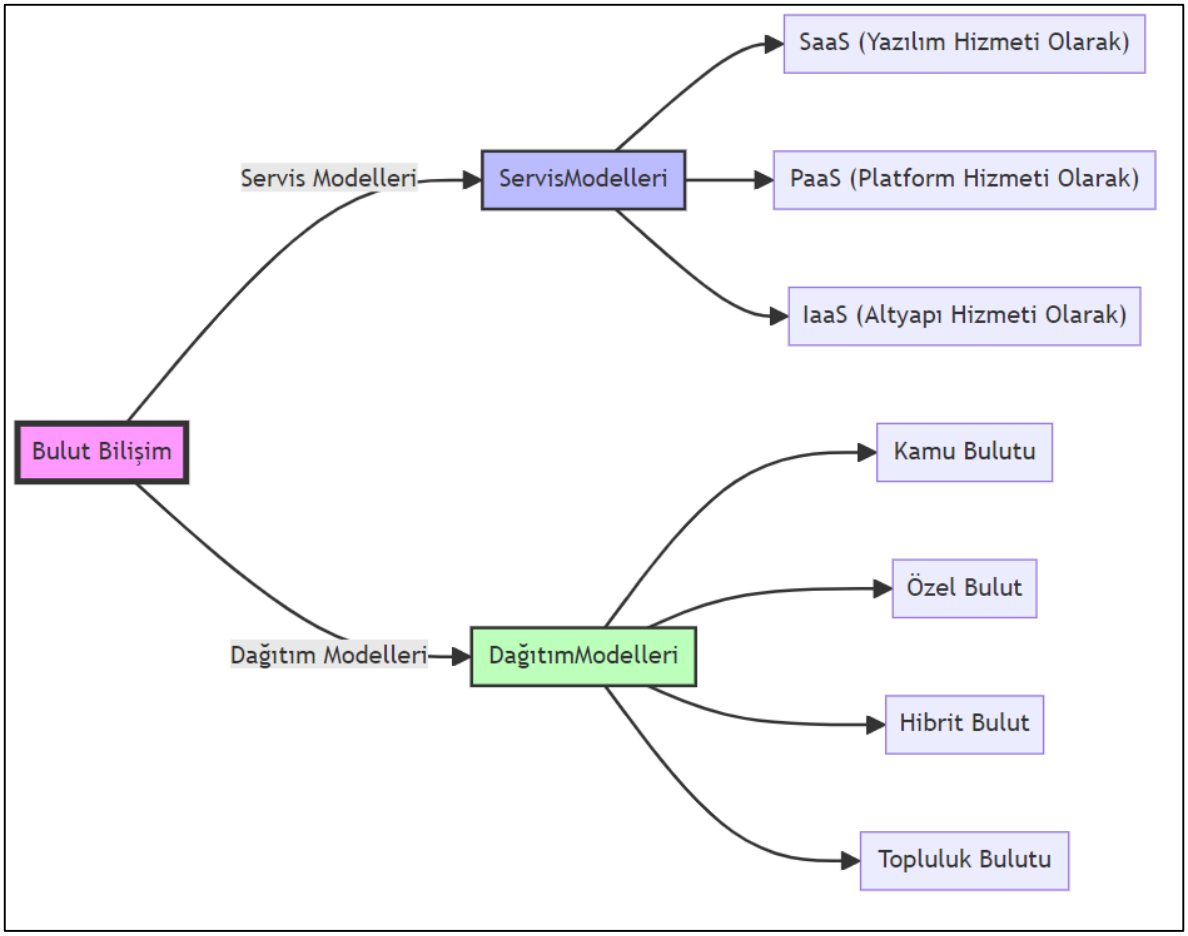
Dawood ve ark (2023) “Bulut Bilişimin Siber Saldırıları ve Güvenliği: Tam Bir Kılavuz” isimli çalışması ile farklı bulut modellerini ve bulut hizmetleri üzerinde tartışmalar yapılmış. Güvenlik trendleri, veri ihlalleri veri gizliliği, veri erişim kontrol edilebilirliği, kimlik doğrulama, yetersiz inceleme, kimlik avı, anahtarların açığa çıkması, denetim ve gizliliğin korunması gibi güvenlik sorunlarına değinmiş ve bu güvenlik sorunlarına karşı önlemler önerilirmiştir.

Singh (2022) “Dijital Çağda Bulut Bilgisayar Güvenliği İçin Blokzinciri Uygulaması” isimli çalışması ile gizlilik, özgünlük ve bütünlük alanlarında bilgi teknolojilerinde önemli bir güvenlik aracı haline gelen blokzinciri teknolojisinin bulut bilişim üzerinde uygulanabilirliğini tartışmıştır.

Abiodun ve ark (2023) “Bulut Bilişim Sistemlerinde Veri Güvenliğini Artırmak İçin Hibrit Kriptografi Kullanan Çift Aşamalı Şifreleme Düzeninin Analizi” isimli çalışma ile bulut tabanlı sistemlerdeki güvenlik açıklarını ortadan kaldırmak için kriptografi yaklaşımı ele alınmıştır. Dosyaları şifrelemek için Şifreleme Yönetimi(RSA) ve şifrelenen dosyaları şifrelemek için Gelişmiş Şifreleme Standardı(AES) kullanılarak Çift aşamalı şifrelemenin tek aşamalı şifrelemeye göre daha avantajlı olduğu yapılan testlerde gösterilmiştir.

2. Bulut Bilişim Mimarisi

Bulut Bilişim Mimarisi, Amazon, Salesforce, Google, IBM, Microsoft ve ark. gibi çeşitli şirketler tarafından sunulan çeşitli bulut bilişim hizmetlerinin yapılandırılmasını ve organizasyonunu ifade eder. Bu hizmetler, e-posta, depolama, hizmet olarak altyapı (IaaS), hizmet olarak yazılım (SaaS) ve daha fazlasını içeren geniş bir yelpazeyi kapsar. Bulut bilişimin cazibesi büyük şirketlerle sınırlı değil; aynı zamanda yeni kurulan girişimleri, girişimcileri, orta ölçekli işletmeleri ve küçük işletmeleri de kapsar. Onlara benzeri görülmemiş fırsatlar ve seçenekler sunarak potansiyel olarak önemli maliyet tasarrufları sağlar. Bulut bilişim aracılığıyla kuruluşlar, tamamı internet üzerinden birbirine bağlı olan büyük bulut sağlayıcılarından yalnızca temel bilgi işlem gücünü, iletişim kapasitesini ve depolama alanını kiralamayı tercih edebilir (Krishna ve ark., 2016).



Şekil 1. Bulut bilişimin şematik tanımı

Bulut hizmeti sağlayıcıları genellikle üç ana gruba ayrılan hizmetler sunar: Hizmet olarak altyapı (IaaS), Hizmet olarak platform (PaaS) ve Hizmet olarak yazılım (SaaS)(Vasiljeva ve ark., 2017). Şekil 1’de bulut bilişim modelleri gösterilmektedir.

Bu kategoriler, bulut bilişim sağlayıcıları tarafından sunulan çeşitli hizmet katmanlarını kapsar. PaaS, bulut bilişimin üç hizmet modelinden biri olarak, SaaS ve IaaS modelleri arasında yer alır ve her ikisine de bağımlıdır. IaaS,

uygulama geliştirme, dağıtım ve barındırma ortamları (PaaS) için gereken fiziksel hesaplama yeteneklerini sağlar, bu da bir SaaS uygulamasını barındırmak için gereklidir. PaaS, kullanıcı tercihlerine bağlı olarak genel, özel veya karma bulut hizmetleri olarak dağıtılabilir.

2.1. Servis modelleri

- **Hizmet Olarak Yazılım (SaaS**): Bu model, tüketicilere, sağlayıcının bulut altyapısı üzerinde çalışan uygulamalarına, web tarayıcıları veya program arayüzleri gibi ince istemci arayüzleri aracılığıyla çeşitli istemci cihazları aracılığıyla erişilebilmesini sağlar (Almorsy ve ark., 2016). Tüketiciler genellikle temeldeki bulut altyapısını yönetmez veya kontrol etmez.

- **Hizmet Olarak Platform (PaaS):** Bu modelde bulut sağlayıcıları, müşterilerin bu platformları veya destek araçlarını yerel olarak kurmalarına gerek kalmadan kendi uygulamalarını geliştirmelerine, dağıtmalarına ve yönetmelerine olanak tanıyan platformlar, araçlar ve diğer hizmetleri sunar (Isharufe ve ark., 2020). Tüketiciler temeldeki bulut altyapısını yönetmezler ancak dağıtılan uygulamalar üzerinde kontrole sahiptirler

- **Hizmet Olarak Altyapı (IaaS):** Tüketiciye sağlanan yetenek, tüketicinin işletim sistemleri ve uygulamaları içerebilecek isteğe bağlı yazılımları dağıtabileceği ve çalıştırabileceği işleme, depolama, ağlar ve diğer temel bilgi işlem kaynaklarının sağlanmasıdır. Sunucular, depolama sistemleri, anahtarlar, yönlendiriciler ve diğer sistemler bir araya getirilerek uygulama bileşenlerinden yüksek performanslı bilgi işlem uygulamalarına kadar uzanan iş yüklerini yönetebilecek hale getirildi (Krishna B. H. ve ark., , 2016). Tüketici, temeldeki bulut altyapısını yönetmez veya kontrol etmez; ancak işletim sistemleri, depolama ve dağıtılan uygulamalar üzerinde kontrole sahiptir; ve muhtemelen belirli ağ bileşenlerinin (örneğin, ana bilgisayar güvenlik duvarları) sınırlı kontrolüne sahiptir.

2.2. Dağıtım Modelleri

Bulut bilişimdeki dağıtım modelleri, bulut hizmetlerinin uygulandığı ve kullanıcılara sunulduğu farklı yolları ifade eder. Dört ana dağıtım modeli vardır (Bouayad ve ark., 2012; Bohn ve ark., 2011):

- **Özel Bulut**: Belirli bir kuruluşa ayrılmış, kuruluşun kendisi, üçüncü bir taraf veya her ikisinin bir kombinasyonu tarafından sahip olunan, yönetilen ve işletilen bir bulut platformu. Tesis içinde veya dışında bulunabilir (Mell ve Grance, 2010).

- **Genel Bulut:** Tüm kullanıcıların kullanımına açık(Amalarethinam ve Rajakumari, 2019), genellikle bir işletme, akademik veya devlet kuruluşunun sahip olduğu, yönettiği ve işlettiği bir bulut platformu (Mell ve Grance, 2010).

- **Topluluk Bulutu**: Görev, güvenlik gereksinimleri veya uyumluluk hususları gibi ortak endişeleri olan belirli bir tüketici topluluğu tarafından özel kullanım için sağlanan bir bulut platformudur. Topluluktaki kuruluşlar veya üçüncü şahıslar tarafından sahiplenilebilir, yönetilebilir veya işletilebilir (Mell ve Grance, 2010).

- **Hibrit Bulut**: Veri ve uygulama taşınabilirliğine olanak tanıyan, standart veya özel teknolojiyle birbirine bağlanan iki veya daha fazla farklı bulut altyapısının (özel, topluluk veya genel) birleşimidir (Mell ve Grance, 2010).

2.3. Avantaj ve Faydalar

Bulut bilişim kuruluşlara çok sayıda avantaj sunar. İlk olarak, işletmelerin yalnızca kullandıkları kaynaklar için ödeme yapmalarına izin vererek maliyet verimliliği sağlar, böylece ön altyapı yatırımı gerekliliğini azaltır ve potansiyel olarak genel maliyetleri düşürür. İkinci olarak, bulut hizmetleri ölçeklenebilirlik sunarak kuruluşların talebe göre kaynakları kolayca yukarı veya aşağı ölçeklendirmesine olanak tanır, aşırı provizyona gerek kalmadan optimum performansı ve kaynak kullanımını sağlar. Ayrıca bulut bilişim, belirli iş ihtiyaçlarına ve tercihlerine uyacak çeşitli hizmet modelleri ve dağıtım seçenekleri sunarak esneklik sağlar ve kuruluşların bulut ortamlarını buna göre uyarlamasına olanak tanır. Üstelik bulut bilişim, kapsamlı altyapı kurulumu ve yönetimi yükü olmadan en son teknolojilere ve hizmetlere erişim sağlayarak yenilikçiliği teşvik eder, işletmelerin hızla yenilik yapmasına ve sürekli gelişen pazar ortamında rekabetçi kalmasını sağlar (Isharufe ve ark., 2020; Bohn ve ark., 2011; Popli ve Gagandeep, 2019) .

3. Bulut Bilişimde Tehdit Türleri

• **Hizmet Hırsızlığı Saldırıları**: Bir hizmet sağlayıcı ödeme yapmadan gerekli yetkilendirme alanmadan hizmetlerden yararlanmayı veya kötüye kullanmayı amaçlayan çeşitli kötü niyetli faaliyetleri ifade eder (Yan ve Yu, 2015).

• **Hizmet Reddi (DoS) Saldırıları:** Hizmet Reddi (DoS) saldırıları, bulut kaynaklarını aşırı yükleyerek veya güvenlik açıklarından yararlanarak bulut hizmetlerinin kullanılabilirliğini bozmak ve böylece saldırı sırasında kullanıcıların verilerine erişmesini engellemek anlamına gelir (Yan ve Yu, 2015).

• **Kötü Amaçlı Yazılım Ekleme Saldırıları(Malware):** Bulutta çalışan sanal makinelerle veya buluta güç veren sistemlerle birlikte çalışmak üzere tasarlanmış bir sisteme yapılan yazılım eklemeleridir. Bulutta veri trafiğinin izlenmesi veya saldırganlara erişim izni verilmesi gibi çeşitli amaçlarla işlevsel değişiklikler yapılabilir. Başarılı olursa, gerçek kullanıcı verileri kötü amaçlı yazılım geliştiricisi tarafından ele geçirilebilir (Amira ve ark., 2024).

• **Hedefli Paylaşılan Bellek Saldırıları**: Fiziksel ve sanal makineler arasında paylaşılan bellek önbelleklerinden veya birincil bellekten yararlanarak potansiyel olarak yan kanal saldırılarına ve kötü amaçlı yazılım enjeksiyonlarına yol açar (Amara ve ark., 2017).

• **Kimlik Avı Saldırıları:** Bir savunma görevi gören anti-spam yazılımıyla, kullanıcıları kimlik bilgilerini ifşa etmeleri için kandırmak amacıyla web bağlantılarının manipüle edilmesini içerir (Amara ve ark., 2017).

• **Atlama Taşı Saldırıları**: Saldırıları aracı ana bilgisayarlar aracılığıyla yönlendirerek ve genellikle anonimlik için yasa dışı botnet'lerden yararlanarak saldırganların kimliklerini gizlemeyi amaçlar (Ramanathan ve ark., 2011).

• **Ses Steganografi Saldırıları:** Daha az göze çarpan alanları ustalıkla değiştirerek, bulut depolama da dahil olmak üzere medya dosyalarındaki gizli verileri gizler ve kötü niyetli kişilerin hassas bilgileri gizlice iletmesine olanak tanır (Liu ve ark., 2011).

• **Sanal Makinelere (VM'ler) ve Hiper Yöneticilere (HV'ler) Yönelik Saldırılar:** Bunlar Sanal Makineleri (VM'ler) ve Hiper Yöneticileri (HV'ler) hedef alan çeşitli saldırı türleridir. Sanal ortamda güvenlik tehditleri, geleneksel tehditlerin yanı sıra benzersiz riskler de içerir. Bu tehditlerin bazıları şunlardır: (Luo ve ark.,2011)

VM'ler ve VMM Arasındaki Saldırılar: Sanal makine (VM) ortamında izolasyonun yanlış yapılandırılması veya uygun olmayan erişim kontrol politikalarının uygulanmaması durumunda, VM'ler arasında veya VM'ler ile Sanal Makine Monitörü (VMM) arasında saldırılar gerçekleşebilir. Bu tür saldırılar, sistemin bütünlüğünü ciddi şekilde tehlikeye atabilir.

VM Kaçışı: VM kaçışı, bir VM'de çalışan kodun, hipervizörle etkileşim kurarak VM içindeki işletim sisteminden kaçmasına olanak tanır. Bu tür bir saldırı, ana işletim sistemi ve o ana bilgisayar üzerinde çalışan diğer VM'ler de dahil olmak üzere tüm sistem üzerinde kök erişim sağlayabilir. VM kaçışı, sanal makine izolasyonunun ciddi şekilde ihlal edildiği en kötü senaryolardan biridir.

Ana Bilgisayarın VM'leri Kontrolü: Ana bilgisayar, sanal makineleri kontrol eder ve başlatma, durdurma, kaynakları değiştirme ve VM uygulamalarını izleme gibi yetkilere sahiptir. Ayrıca, VM'lerle ilişkili ağ trafiği de ana bilgisayardan geçer. Bu durum, ana bilgisayarın tehlikeye girmesi halinde VM'lerin güvenliğini riske atar.

• **Ortadaki adam (MITM):** Bu saldırı, kullanıcının makinesindeki iletişimi gizlice dinlemek için kullanılır. Bu saldırı, yeterli güvenlik önlemlerine sahip sertifikaların kullanılmamasından kaynaklanmaktadır (Zawaideh ve ark., 2022).

• **Sybil Saldırısı:** Sybil saldırıları, kötü niyetli aktörlerin ağın işlevselliğini manipüle etmek için sahte kimlikler kullandığı ve genellikle orijinal düğümleri tehlikeye atılmış düğümlere dönüştürdüğü bulut bilişim ortamlarında önemli bir tehdit oluşturur. Bir yer paylaşımlı ağ içinde çalışan Sybil düğümleri, mantıksal düğümlerin önemli bir kısmı üzerinde kontrol uygulayabilir ve böylece başarılı bir sızma durumunda potansiyel olarak tüm ağın kontrolünü ele geçirebilir (Dawood. ve ark., 2023).

• **Kara Delik Saldırısı:** Bir tür hizmet reddi saldırısıdır. Paketleri teslim etmesi gereken bir yönlendiricinin kasıtlı olarak görevini yerine getirmemesi durumunda ortaya çıkar. Sonuç olarak, iletilen mesajlar doğru varış noktasına alınamaz ancak düşürülerek paket kaybına neden olur (Malik T. S.ve ark., 2023).

• **Solucan Deliği Saldırısı:** Solucan deliği saldırısı, kötü niyetli düğümlerin bir düğümden gelen paketleri yakalayıp bunları ağdaki başka bir konuma ileterek iki kötü niyetli düğüm arasında kısa bir yol olduğu yanılsamasını

yarattığı bir tür güvenlik ihlalidir. Ele geçirilen bu paket daha sonra ağ içinde yeniden yürütülür ve bu da yanlış/sahte yönlendirme bilgilerine, ağ topolojisinin değişmesine ve potansiyel paket kaybına yol açar. Bu yanıltıcı davranış, ağ üzerinden büyük miktarda veri akışını çekerek, kötü niyetli düğümlerin seçici paket atma gibi daha fazla güvenlik saldırıları başlatmasına olanak tanır, böylece yönlendirme ve veri toplama gibi normal ağ işlevlerini bozar. (Guo J. ve Lei Z, 2011; Dwivedi ve ark, 2019)

4. Bulut Bilişim Tehditlere Karşı Olası Çözümler

• **Erişim kontrolleri,** fiziksel güvenliği sağlamak için kullanılan çeşitli önlemleri içerir. Bu önlemler, video gözetimi ve çevre düzenlemeleri gibi araçları kapsar ve genellikle veri merkezlerindeki fiziksel altyapıyı ve bulut kaynaklarını korumak için uygulanır (Kumar ve ark., 2023).

• **Ağ güvenliği**, ağları ve verilerini yetkisiz erişimden, siber saldırılardan ve diğer güvenlik ihlallerinden korumak için çeşitli teknolojilerin, süreçlerin ve politikaların uygulanmasıdır. Güvenlik duvarları, sızma tespit ve önleme sistemleri (IDPS), sanal özel ağlar (VPN'ler), erişim kontrolü, şifreleme, yama yönetimi, güvenlik farkındalık eğitimi, ağ bölümlendirme, düzenli güvenlik denetimleri ve olay yanıt planı gibi yaygın güvenlik önlemleri, ağ güvenliğini artırmak için kullanılır. Bu önlemlerin bir araya getirilmesi ve sürekli olarak gelişen tehditlere karşı dikkatli olunması, organizasyonların ağ güvenliğini güçlendirmesine ve değerli varlıklarını siber tehditlerden korumasına yardımcı olur. (Jangjou M. ve Sohrabi M.K, 2022; Zhou ve ark, 2022)

• **Kimlik ve Erişim Yönetimi (IAM)**, Kimlik ve Erişim Yönetimi (Identity and Access Management - IAM), bir organizasyonun bilişim altyapısındaki dijital kimlikleri ve kaynaklara erişimi yönetmek ve denetlemek için kullandığı bir çerçeve veya süreçler bütünüdür. IAM sistemleri, yalnızca yetkilendirilmiş bireylerin veya varlıkların belirli kaynaklara, uygulamalara veya verilere erişimine izin verirken aynı zamanda güvenliği, gizliliği ve düzenlemelere uyumu sağlamak için tasarlanmıştır. IAM genellikle aşağıdaki temel işlevleri içerir: Kimlik Doğrulama, kullanıcının kimliğini doğrulama sürecidir; Yetkilendirme, kullanıcılara verilen izinleri ve ayrıcalıkları tanımlar; ve Denetleme, kullanıcı etkinliklerini izleme ve kaydetme sürecidir. IAM sistemleri, kullanıcı kimliklerini yönetmek, erişim kontrollerini uygulamak ve kullanıcı etkinliklerini izlemek suretiyle dijital kaynakların güvenliğini, gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için önemli bir rol oynarlar. Bilgi teknolojisi ortamlarının giderek karmaşıklaşması, bulut hizmetlerinin yükselmesi ve düzenleyici uyum ihtiyacı, IAM'ın organizasyonların hassas bilgilerini korumak ve siber güvenlik risklerini azaltmak için önemli hale gelmesine neden olmuştur. (Sikarwar ve ark, 2024;Aboukadri ve ark, 2024)

• **Veri yedekleme ve felaket kurtarma sistemleri,** bilgi teknolojisi altyapısının temel bileşenlerindendir ve veri kaybını önlemek ve iş sürekliliğini sağlamak amacıyla tasarlanmıştır. Örneğin, merkezi yedekleme sistemleri, birden fazla katmanlı bir yapıya sahip olup istemci PC'lerinde yedekleme ajan yazılımı, yönetim sunucusu, veri kopyalama sunucusu ve yedekleme cihazlarından oluşur. Anlık görüntüler, hızlı yedekleme ve geri yükleme imkanı sağlar ve genellikle büyük politika çerçevesinde kullanılır. Felaket kurtarma sistemleri arasında uzak yedekleme depolama önemli bir yer tutar çünkü felaket durumlarında veri kaybını azaltır. Güvenlik duvarları ve doğrulama çerçeveleri ise veri bütünlüğünü sağlamak için kullanılır. Bu sistemler, iş sürekliliğini korumak ve veri bütünlüğünü sağlamak için hayati öneme sahiptir. Bunların düzenli olarak test edilip güncellenmesi de kritik önem taşır. (Singh ve Battra, 2023)

• **Güvenlik Açığı Koruması ve Yönetimi,** Bulut hizmet sağlayıcısı aracılığıyla yama yönetiminde iyileştirmeler yapılması çok önemlidir. Potansiyel erişim noktalarını en aza indirmek ve bulut tabanlı korsan saldırılarının olasılığını azaltmak için sürekli güncellemeler ve bakımlarla birlikte düzenli güvenlik açığı değerlendirmeleri yapılmalıdır. Hizmet sağlayıcı tarafından bir İzinsiz Giriş Tespit Sisteminin (IDS) uygulanması, bulut hizmetinin emniyetini ve güvenliğini garanti etmek için çok önemlidir (Alrasheed ve ark., 2022).

• **Güvenlik Denetimi ve Uyumluluk,** endüstri standartlarına ve yönergelerine uygunluğu sağlamak için düzenli kontrolleri ve değerlendirmeleri kapsar. Buna, bağımsız denetimler ve sertifikalar yoluyla bulut hizmet sağlayıcılarının (CSP'ler) güvenlik önlemlerinin değerlendirilmesi de dahildir. Fiziksel Güvenlik, fiziksel altyapıyı ve bulut kaynaklarını barındıran veri merkezlerini korumak için erişim kontrollerinin, video gözetiminin ve çevresel önlemlerin uygulanmasını içerir (Kumar ve ark., 2023).

• **Veri şifreleme,** ister saklansın ister aktarılsın, hassas bilgilerin yetkisiz erişime veya müdahaleye karşı korunması için hayati öneme sahiptir. Atıl durumdaki şifreleme, güvenliği korumak için AES gibi güçlü algoritmalar ve katı anahtar yönetimi uygulamaları kullanarak verilerin depolama cihazlarında okunamaz halde kalmasını sağlar. Aktarım sırasındaki şifreleme, müdahaleyi önlemek için SSL/TLS gibi protokolleri kullanarak ağlar arasındaki hareket

sırasında verileri korur. Güçlü şifreleme tekniklerinin ve güvenli anahtar yönetimi uygulamalarının kullanılması, şifre çözme girişimlerini engellemek ve veri güvenliğini korumak için çok önemlidir. Kuruluşlar bu uygulamalara bağlı kalarak veri gizliliğini ve bütünlüğünü geliştirebilir, ihlal ve yetkisiz ifşa riskini azaltabilir (Raghav ve ark.,2023)

• **Güvenlik İzleme ve Günlüğe Kaydetme,** Sistemde gerçekleşen tüm erişim ve işlemlerin kaydedilmesi ve izlenmesi, güvenlik açısından önemlidir. Bu sayede olası güvenlik ihlalleri tespit edilebilir. (Teegala ve ark, 2023)

SIEM (Güvenlik Bilgileri ve Olay Yönetimi) gibi teknolojilerin kullanılması, çeşitli bulut hizmetlerinden günlüklerin toplanıp analiz edilmesini sağlayarak tehdit algılama yeteneklerini önemli ölçüde artırır.

Tablo 1. Bulut bilişimdeki farklı saldırı türlerine yönelik çeşitli önlemlerin kullanımını

Saldırı Türü	**Önlem**
Hizmet Hırsızlığı Saldırıları	Kimlik ve Erişim Yönetimi (IAM), Güvenlik Açığı Koruması ve Yönetimi
Hizmet Reddi (DoS) Saldırıları	Ağ Güvenliği, İzinsiz Giriş Tespit ve Önleme Sistemleri (IDPS)
Kötü Amaçlı Yazılım Ekleme Saldırıları	Güvenlik Açığı Koruması ve Yönetimi, Güvenlik İzleme ve Günlüğe Kaydetme
Hedefli Paylaşılan Bellek Saldırıları	Erişim Kontrolleri, Güvenlik Açığı Koruması ve Yönetimi
Kimlik Avı Saldırıları	Erişim Kontrolleri, Son Kullanıcı Güvenliği, Güvenlik İzleme ve Günlüğe Kaydetme
Atlama Taşı Saldırıları	Ağ Güvenliği, Kimlik ve Erişim Yönetimi (IAM)
Ses Steganografi Saldırıları	Veri Şifreleme, Güvenlik İzleme ve Günlüğe Kaydetme
Sanal Makinelere ve Hiper Yöneticilere Yönelik Saldırılar	Kimlik ve Erişim Yönetimi (IAM), Ağ Güvenliği
Ortadaki Adam (MITM)	Ağ Güvenliği, Veri Şifreleme
Sybil Saldırısı	Kimlik ve Erişim Yönetimi (IAM), Güvenlik Açığı Koruması ve Yönetimi
Kara Delik Saldırısı	Ağ Güvenliği, Güvenlik İzleme ve Günlüğe Kaydetme
Solucan Deliği Saldırısı	Ağ Güvenliği, İzinsiz Giriş Tespit ve Önleme Sistemleri (IDPS)

• **Son Kullanıcı Güvenliği**, son kullanıcı cihazlarının çeşitli güvenlik tehditlerine karşı korunması açısından hayati öneme sahiptir. Kötü amaçlı yazılım bulaşmalarını algılayan ve kaldıran antivirüs yazılımı ve gelişmiş tehdit algılama ve yanıt yetenekleri sağlayan Uç Nokta Tespit ve Yanıt (EDR) çözümleri de dahil olmak üzere birçok temel bileşeni kapsar. Mobil Cihaz Yönetimi (MDM) çözümleri, kurumsal kaynaklara erişen mobil cihazları yönetir ve güvence altına

alır, güvenlik politikalarını uygular ve uzaktan yönetim özelliklerini etkinleştirir. En iyi uygulamalar arasında düzenli güncellemeler, güvenlik tehditleri konusunda kullanıcı eğitimi, güvenlik politikalarının uygulanması için uç nokta yapılandırması ve uç nokta etkinliklerinin sürekli izlenmesi yer alır. Güçlü uç nokta güvenlik önlemleri, kuruluşların kötü amaçlı yazılımlara, yetkisiz erişime ve veri ihlallerine karşı korunmasına yardımcı olarak kurumsal verilerin ve kaynakların güvenliğini sağlar.

Tablo 1'de, bulut bilişimdeki farklı saldırı türlerine yönelik çeşitli önlemlerin kullanımını ilişkin bilgiler yer almaktadır.

5. Bulut Bilişimde Tehditlere Karşı Yapay Zeka Sistemlerinin Kullanımı

Yapay zeka, çalışmayı kolaylaştırmak, tekrarlanan görevleri otomatik olarak gerçekleştirmek ve sorunları kendi başına denetleyip düzeltmek için bulut sistemlerine yerleştirilmektedir (Mohammed ve ark., 2023). Google, Amazon, Microsoft ve IBM gibi teknoloji devleri bulutta yapay zeka sistemleri uygulayarak makine öğrenimi platformları ve gelişmiş metin analizi, çeviri, akıllı arama, dil işleme ve bilgi yönetimi gibi çeşitli yapay zeka hizmetleri sunmaktadır. Yapay zekanın bulut hizmetlerine bu entegrasyonu, bulut bilişimin bir sonraki evrimini temsil ederek işlevsellik ve performansı artıracağı düşünülmektedir (Kumar, 2016).

5.1. Proaktif tehdit izleme ve tespiti

Anomali tespiti, ağ trafiğindeki alışılmadık veya potansiyel olarak zararlı davranışları tespit etmek için kullanılan bir tekniktir. Bu teknik, normal ağ trafiği modelleri üzerine kurulmuş istatistiksel veya makine öğrenimi tabanlı yöntemler kullanarak ağdaki anormallikleri belirlemeyi amaçlar. Anomali tespiti, ağ güvenliği alanında önemli bir rol oynar çünkü potansiyel saldırıları veya diğer istenmeyen olayları erken aşamada tespit ederek ağın güvenliğini artırır. Bu sayede ağ yöneticileri, olası tehditlere karşı daha hızlı ve etkili önlemler alabilirler. (Thatte ve ark., 2011)

Tehdit İstihbaratı: AI, çeşitli kaynaklardan gelen tehdit istihbaratını toplayıp analiz ederek, bilinen tehditlerin yanı sıra sıfırıncı gün saldırılarına karşı da koruma sağlayabilir (Khorshed ve ark., 2012).

5.2. Davranışsal analiz

Kullanıcı ve Cihaz Davranışlarını İzleme: Yapay zeka, kullanıcıların ve cihazların davranış modellerini sürekli olarak öğrenir ve analiz eder. Bu sayede, yetkisiz erişim veya iç tehditler gibi potansiyel güvenlik ihlallerini ortaya çıkarabilir (Patel ve ark., 2012; Khorshed ve ark., 2012).

5.3. Otomatik yanıt ve düzeltme mekanizmaları

Otomatik Düzeltme; Yapay zeka sistemleri, tehditleri tespit ettiğinde otomatik olarak yanıt verebilir. Bu, zararlı yazılımların izolasyonu, tehlikeli trafiğin engellenmesi veya güvenlik yapılandırmalarının dinamik olarak ayarlanması şeklinde olabilir. Sürekli Güncelleme ve Öğrenme; Yapay zeka, güvenlik olaylarından öğrenerek ve güvenlik politikalarını sürekli olarak güncelleyerek, gelecekteki tehditlere karşı daha iyi koruma sağlar (Patel ve ark., 2012).

Bulut servislerine sahip teknoloji devleri de siber saldırılarla ve veri ihlalleriyle karşı karşıyadır. Yapay zekanın kullanılması, bulut uygulamalarında depolanan önemli kurumsal verilere yetkisiz erişimin önlenmesine yardımcı olur (Tadeo ve ark., 2021). Yapay zeka modelleri, özellikle değişen bir ortamda bilgisayar ağlarının kötü niyetli kullanımı riskleriyle baş etmede, bilgi güvenliği sorunlarını çözmeye yardımcı olur (Surya, 2018). Yapay zeka bulut bilişim güvenliğnide verileri işlemek ve otonom kararlar vermek için kullanılmaktadır. Bu durum daha hızlı ve daha yetenekli karar alma olanağı sunmaktadır(Du, 2022).

6. Sonuç

Yapay zeka (AI), gelişmiş tehdit algılama, risk yönetimi ve hızlı yanıt yetenekleri sağlayarak bulut bilişim güvenliğini güçlendirmede önemli bir rol oynar. Siber tehditlerin artan karmaşıklığı ve bulut ortamlarında dolaşan büyük miktarda veri göz önüne alındığında, yapay zeka destekli çözümler, anormallikleri ve potansiyel ihlalleri gerçek zamanlı olarak belirlemede benzersiz verimlilik ve etkinlik sunar. Yapay zeka, makine öğrenimi algoritmaları ve tahmine dayalı analitikler aracılığıyla, güvenlik önlemlerini dinamik bir şekilde uyarlamak için kalıpları ve davranışları

sürekli olarak analiz edebilir ve ortaya çıkan riskleri daha büyümeden azaltabilir. Üstelik yapay zeka destekli otonom sistemler, güvenlik operasyonlarını düzene sokarak olaylara hızlı tepki verilmesini ve iyileştirme yapılmasını sağlıyor, böylece bulut altyapılarının gelişen siber tehditlere karşı dayanıklılığını güçlendiriyor. Özünde, yapay zeka teknolojilerinin entegrasyonu yalnızca bulut ortamlarının genel güvenlik duruşunu geliştirmekle kalmıyor, aynı zamanda bulut bilişim kaynaklarının tüm potansiyelinden yararlanma konusunda güven veriyor ve bu güveni de güçlendiriyor.

Yapay zeka, sürekli değişen tehdit manzarasını analiz etmek, gerçek zamanlı tehdit algılama ve proaktif yanıt verme yeteneği sunmakla kalmaz, aynı zamanda güvenlik politikalarının otomatik uygulanmasını ve dinamik risk yönetimini de kolaylaştırır. Ancak teknolojinin ilerlemesi, insan faktörünün güvenlikteki önemini azaltmamaktadır; bu nedenle, yapay zeka ve bulut güvenliği konularında eğitim ve farkındalık programlarına yatırım yapmak hayati önem taşır. Gelecekte, yapay zeka tabanlı tehdit algılama sistemlerinin geliştirilmesi, otomatikleştirilmiş güvenlik politikaları ve risk yönetimi çözümlerinin entegrasyonu, ve kapsamlı eğitim programlarının uygulanması, bulut bilişim güvenliğinin ön saflarında yer alacaktır. Bu öneriler, hem akademik hem de endüstriyel araştırmacılar için gelecek çalışmaların yönünü belirlemede kritik bir rol oynayabilir

Kaynaklar

Abiodun M. K., Chioma U., Imoize A. L., Awotunde J. B., Lee C.-C., Adeniyi A. E., Li C.-T. (2023). Analysis of a Double-stage Encryption Scheme Using Hybrid Cryptography to Enhance Data Security in Cloud Computing Systems. Journal of Library and Information Studies.

Aboukadri S., Ouaddah A., Mezrioui A. (2024). Machine learning in identity and access management systems: Survey and deep dive. Computers Security.

Almorsy M., Grundy, J., Müller I. (2016). An Analysis of the Cloud Computing Security Problem. Communication Technologies.

Alrasheed S. H., Aied alhariri M., Adubaykhi S. A., El Khediri S. (2022). Cloud Computing Security and Challenges: Issues, Threats, and Solutions. In 2022 5th Conference on Cloud and Internet of Things.

Amalarethinam D. I. G., Rajakumari S. E. J. (2019). A Survey on Security Challenges in Cloud Computing. Journal of Physical Sciences.

Amara N., Huang Z., Ali A. (2017). Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery.

Amira A., Derhab A., Karbab E. B., Nouali O. (2024). A Survey of Malware Analysis Using Community Detection Algorithms. ACM Computing Surveys.

Bohn R. B., Messina J., Liu F., Tong J. (2011). NIST Cloud Computing Reference Architecture. In 2011 IEEE World Congress on Services.

Bouayad A., Blilat A., Mejhed N. E. H., El Ghazi M. (2012). Cloud computing: Security challenges. In 2012 Colloquium in Information Science and Technology.

Dawood M., Tu S., Xiao C., Alasmary H., Waqas M., Rehman S. U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. Symmetry, November 2023.

Du J. (2022). Analysis of a Joint Data Security Architecture Integrating Artificial Intelligence and Cloud Computing in the Era of Big Data. In 2022 4th International Conference on Smart Systems and Inventive Technology.

Dwivedi R. K., Saran M., Kumar R. (2019). A Survey on Security over Sensor-Cloud. Başlık. 2019 9th International Conference on Cloud Computing, Data Science Engineering (Confluence).

Guo J., Lei Z. (2011). A kind of wormhole attack defense strategy of WSN based on neighbor nodes verification. 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN).

Hasimi L., Zavantis D., Shakshuki E., Yasar A. (2024). Cloud Computing Security and Deep Learning: An ANN approach. Procedia Computer Science.

Isharufe W., Jaafar F., Butakov S. (2020). Study of Security Issues in Platform-as-a-Service (PaaS) Cloud Model. In 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE).

Jangjou, M., Sohrabi, M. K. (2022). A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing. Archives of Computational Methods in Engineering: State of the Art Reviews.

Khorshed M. T., Ali A. B. M. S., Wasimi S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems - The International Journal of Grid Computing and eScience.

Krishna B. H., Kiran S., Murali G., Reddy R. P. K. (2016). Security Issues in Service Model of Cloud Computing Environment. Procedia Computer Science.

Kumar A., Bhardwaj A., Singh A. (2023). A Review of Data Security in Cloud Computing. In 2023 14th International Conference on Computing Communication and Networking Technologies.
Kumar M. (2016). An Incorporation of Artificial Intelligence Capabilities in Cloud Computing. International Journal Of Engineering And Computer Science.
Kumari S., Solanki K., Dalal S., Dhankhar A. (2022). Analysis Of Cloud Computing Security Threats and Countermeasures. In 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions).
Liu B., Xu E., Wang J., Wei Z., Xu L. Z., Zhao B., Su J. (2011). Thwarting audio steganography attacks in cloud storage systems. In 2011 International Conference on Cloud and Service Computing.
Luo S., Lin Z., Chen X., Yang Z., Chen J. (2011). Virtualization Security for Cloud Computing Service. 2011 International Conference on Cloud and Service Computing.
Malik T. S., Siddiqui M. N., Mateen M., Malik K. R., Sun S., Wen J. (2022). Comparison of Blackhole and Wormhole Attacks in CloudMANET Enabled IoT for Agricultural Field Monitoring. SECURITY AND COMMUNICATION NETWORKS.
Mell P., Grance T. (2010). The NIST Definition of Cloud Computing. Communications of the ACM.
Mohammed S., Fang W. C., Ramos C. (2023). Special issue on ‘‘artificial intelligence in cloud computing’’. Computing.
Patel A.,Taghavi M., Bakhtiyari K., J Joaquim. (2012). An Intrusion Detection And Prevention System In Cloud Computing: A Systematic Review. Journal of Network and Computer Applications. 36. 10.1016/j.jnca.2012.08.007.
Popli M., Gagandeep. (2019). A Survey on Cloud Security Issues and Challenges. In 2019 6th International Conference on Computing for Sustainable Global Development.
Raghav; Andola N.; Verma K.; Venkatesan S.; Verma Ş. (2023). Multi-Keyword Searchable and Verifiable Attribute-Based Encryption Over Cloud Data. IEEE Transactions on Cloud Computing.
Ramanathan S., Goel S., Alagumalai S. (2011). Comparison of Cloud database: Amazon's SimpleDB and Google's Bigtable. In 2011 International Conference on Recent Trends in Information Systems.
Sikarwar S., Jeyanthi N., Thandeeswaran R., Mcheick H. (2024). SDS-IAM: Secure Data Storage with Identity and Access Management in Blockchain. International Journal of Performability Engineering.
Singh A. (2022). Blockchain Implication for Cloud Computing Security in the Digital Era. Pranjana: The Journal of Management Awareness.
Singh A., Battra J. (2023). Strategies for Data Backup and Recovery in the Cloud. International Journal of Performability Engineering.
Surya L. (2018). Streamlining Cloud Application with AI Technology. International Journal of Innovations in Engineering Research and Technology.
Tadeo D. A. G., John S. F., Bhaumik A., Neware R., Yamsani N., Kapila D. (2021). Empirical Analysis of Security Enabled Cloud Computing Strategy Using Artificial Intelligence. In 2021 International Conference on Computing Sciences.
Teegala S. P., Vijai C., Nagpal A., Anuradha R., Aljbori A., Swathi B. (2023). Enhanced Authentication Methods for Access and Control Management in Cloud Computing. 10th IEEE Uttar Pradesh Section International Conference on Electrical.
Thatte G., Mitra U., Heidemann J. (2011). Parametric Methods for Anomaly Detection in Aggregate Traffic. IEEE/ACM Transactions on Networking, 2011.
Vasiljeva T., Shaikhulina S., Kreslins K. (2017). Cloud Computing: Business Perspectives, Benefits and Challenges for Small and Medium Enterprises (Case of Latvia). Procedia Engineering.
Yan Q., Yu F. R. (2015). Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine.
Zawaideh F. H., Ghanem W. A. H. M., Yusoff M. H., Saany S. I. A., Jusoh J. A., El-Ebiary Y. A. B. (2022). The Layers of Cloud Computing Infrastructure and Security Attacking Issues. Journal of Pharmaceutical Negative Results, Special Issue.
Zhou Y., Zhao G., Alroobaea R., Baqasah A. M., Miglani R. (2022). Research on data mining method of network security situation awareness based on cloud computing. Journal of Intelligent Systems.