Black Sea Journal of Engineering and Science
doi: 10.34248/bsengineering.1310281

Open Access Journal
e-ISSN: 2619 – 8991

Derleme (Review)
Cilt 6 - Sayı 4: 658-667 / Ekim 2023
(Volume 6 - Issue 4: 658-667 / October 2023)

BULUT SERVİSLERİ VE BULUT GÜVENLİĞİ İÇİN ONTOLOJİ TABANLI HİZMET DÜZEYİ SÖZLEŞMELERİ

Sena YAKUT[1]*, Özgü CAN[2]

[1]*Ege University, Institute of Science and Technology, 35100, İzmir, Türkiye*
[2]*Ege University, Faculty of Engineering, Computer Engineering, 35100, İzmir, Türkiye*

Özet: Bulut bilişim, günümüzdeki en önemli teknolojik gelişim ve dönüşümlerinden biri olarak kabul edilmektedir. Bu teknolojinin gelişmesi ile veri tabanı servislerinin, sunucu ve depolama hizmetlerinin yönetimi ve kullanımı kolaylaşmış ve daha düşük maliyetler ile gerçekleştirilebilir bir hale gelmiştir. Son kullanıcılardan büyük ölçekli işletmelere kadar geniş bir kullanıcı kitlesine sahip olan bulut bilişimin popülerleşmesi bulut güvenliği kaygılarını da beraberinde getirmektedir. Farklı bulut servislerinin farklı hizmet katmanlarını karşılaması, atak yüzeylerinin geleneksel yöntemlerden çok daha fazla olması gibi sebepler, bulut güvenliğinin yönetimini zorlaştırmaktadır. Bulut servislerinin yönetimini ve bulut güvenliğini sağlamak amacı ile, bulut hizmetleri kullanıcılarının ve bulut sağlayıcılarının hizmetlerin güvenlik, kullanılabilirlik, yanıt verme düzeyleri gibi kritik özellikleri garanti eden Hizmet Düzeyi Sözleşmeleri (*Service Level Agreements, SLAs*) bulunur. Bu sözleşmelere uyumluluk ve sözleşme ihlallerin kontrolü üzerine bulut servisleri ve bulut güvenliği için geliştirilen ontoloji yapısı, bulut servisleri ve bulut güvenliği kavramlarının arasındaki ilişkileri tanımlamaktadır. Bu ontolojik tanımlama, SLA'ların daha iyi anlaşılmasını, yönetilmesini ve sürekli kontrol için otomasyonunu sağlamaktadır. Bu çalışmada, bulut servisleri ve bulut güvenliği kapsamında geliştirilen SLA ontolojileri üzerine kapsamlı bir araştırma ve inceleme sunulmaktadır. Gerçekleştirilen çalışma sonucunda, alandaki mevcut durum ve yaklaşımlar incelenerek kullanılan teknolojiler ve gelecek çalışmalara yönelik fırsatlar değerlendirilmektedir.

Anahtar kelimeler: Bulut bilişim, Bulut güvenliği, Ontoloji, Hizmet düzeyi sözleşmesi, Anlamsal ağ

Ontology-Based Service Level Agreements for Cloud Services and Cloud Security

Abstract: Cloud computing is defined as one of the most important technological developments and transformations nowadays. As cloud technology improves, handling and using services like databases, servers, and storage becomes simpler and cheaper. The popularization of cloud computing, which has a wide range of users from end users to large-scale enterprises, also brings cloud security concerns. Different cloud services have the ability to operate across multiple service layers, attack surfaces and scenarios are much more varied than traditional methods. Because of all these, keeping track of cloud security can be hard and complicated. In order to manage cloud services and provide cloud security, cloud users and cloud providers have Service Level Agreements (SLAs) that guarantee critical features of services such as security, availability, and responsiveness levels. Cloud services and cloud security ontology help to be compliant with these documents and control SLA violations by defining the relationships between cloud services and cloud security concepts. This ontological definition enables SLAs to be better understood, managed, and automated for continuous control. In this study, comprehensive research and review on SLA ontologies for cloud services and cloud are presented. As a result of the study, the current situation and approaches in the area are examined. Also, opportunities for future SLA ontology studies are evaluated.

Keywords: Cloud computing, Cloud security, Ontology, Service Level Agreement, Semantic network

***Sorumlu yazar (Corresponding author):** Ege University, Institute of Science and Technology, 35100, İzmir, Türkiye
E mail: senayktt@gmail.com (S. YAKUT)
Sena YAKUT https://orcid.org/0000-0002-4666-7770
Özgü CAN https://orcid.org/0000-0002-8064-2905

Gönderi: 06 Haziran 2023 **Received:** June 06, 2023
Kabul: 26 Ağustos 2023 **Accepted:** August 26, 2023
Yayınlanma: 15 Ekim 2023 **Published:** October 15, 2023

Cite as: Yakut S, Can Ö. 2023. Ontology-based service level agreements for cloud services and cloud security. BSJ Eng Sci, 6(4): 658-667.

1. Giriş

Bulut bilişim teknolojisi, 21. yüzyılın en önemli teknolojik gelişimi ve dönüşümlerinden biridir. Temel olarak bulut bilişim, kullanıcılarının internet erişiminin olduğu herhangi bir yerden ve herhangi bir zamanda kaynaklarını kullanabileceği ve diğer kullanıcılarla paylaşabileceği hizmet olarak tanımlanmaktadır. Bulut bilişim teknolojisi ile, kullanıcılar tarafından her yerden erişilebilen, herkesle paylaşılabilen veriler ve uygulamalar oluşturulmakta ve kolayca kullanılmaktadır. Bulut bilişimin popülerleşmesinin temel sebebi, geleneksel yöntemlere göre birçok kolaylık ve avantaj sağlamasıdır. Bu kolaylıklar, maliyet, hız, küresel ölçeklendirilebilirlik, verimlilik, performans, güvenilirlik (reliability) ve güvenlik olarak listelenmektedir (Avram, 2014).

Bulut bilişimin popülerleşmesi ile, bulut güvenliği de önem kazanmıştır. Bulut güvenliği, bulut tabanlı servislere gerçekleşebilecek olan potansiyel siber saldırılara karşı sistemleri güçlendirmek için alınmış önlemler, oluşturulmuş kurallar bütünü olarak tanımlanmaktadır (Singh ve ark., 2017). Bulut güvenliği

ile ilgili sorumluluklar, bulut sağlayıcısının sorumlulukları ve bulut hizmeti kullanıcılarının sorumlulukları olarak ikiye ayrılmıştır. Bu ayrıma paylaşılan sorumluluk modeli (*shared responsibility model*) adı verilmektedir. Bu modele göre, her iki taraf da sorumluluklarını bilip bulut tabanlı siber ataklara karşı önlemler ve koruma çözümleri geliştirmekle yükümlüdür.

Hizmet düzeyi sözleşmesi (Service Level Agreement., SLA), bulut hizmetleri sağlayıcısı ve hizmet kullanıcısı arasında hizmetlerin güvenilirlik, kullanılabilirlik ve yanıt verme düzeylerini garanti eden, bir hizmet kesintisi olduğunda kimin yöneteceğini belirten ve belirtilen hizmetlerin düzeyleri karşılanmazsa konuyla ilgili yaptırım süreçlerini açıklayan sözleşmelerdir (Baset, 2012). Güvenlik tabanlı hizmet düzeyi sözleşmesi (*Security Based Service Level Agreement*) ise, bir bulut hizmeti sağlayıcısı ve bulut hizmetleri kullanıcısı arasında bulut hizmetlerinin güvenliği ile ilgili parametrelerin, metriklerin ve standartların tanımlandığı sözleşmelerdir. Bu tanımlamalara ek olarak, güvenlik standartlarına uyulmadığı durumda uygulanacak süreçlerin tanımlamalarını da kapsar. Bazı şirketler ve bulut sağlayıcıları tarafından güvenlik tabanlı SLA, SLA'ların bir parçası olarak belirlenmektedir. Bulut servisleri, bulut güvenliği SLA'nın birlikte düşünülüp, bir arada değerlendirilmesi oldukça önemlidir. Bulut hizmeti kullanıcılarının, sağlayıcılar tarafından paylaşılmış SLA dokümanlarını referans alarak net beklentileri oluşmaktadır. Örneğin, bir bulut hizmeti kullanıcısı, bir güvenlik servisinin her ayın %99,99'luk zaman diliminde sorunsuz şekilde çalışacağından emin olmak isteyecektir. Bulut sağlayıcısı ve bulut hizmeti kullanıcısının arasındaki SLA'lara ek olarak, bulut hizmeti kullanılarak oluşturulmuş bütün uygulamalar ve bu uygulama kullanıcıları arasında da SLA olması kaçınılmazdır.

SLA sözleşmeleri, performans başarısı, servis erişim hızı, hizmet çıktıları, hizmet takibi ve raporlama gibi detaylara sahiptir. Güvenlik tabanlı SLA dokümanlarında ise, bulut hizmetleri kullanılarak oluşturulmuş olan uygulamaların güvenliği, zafiyet yönetimi, güvenlik testleri, statik ve dinamik kod analizi, mimari güvenliği, siber olaylara müdahale ve analiz gibi başlıklara değinilmekte, bu sayede uygulama kullanıcıları da bu SLA'lardan uygulama güvenliği ile ilgili bilgi sahibi olabilmektedir.

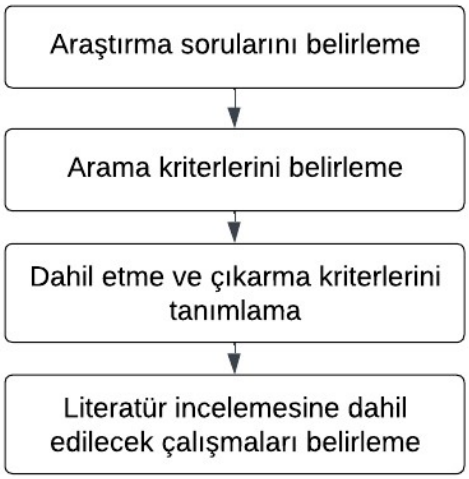
SLA'ların bulut servisleri ve bulut güvenliği ile değerlendirilebilmesi için, otomasyon kurulması esastır. Bu gerekliliği karşılayabilmek için geliştirilebilecek ontolojik bir yapı, belirli bir alanda kavramlar ve ilişkileri sistemli bir şekilde tanımlar (Ontology, 2023). SLA'ların geliştirilmesinde ontoloji tabanlı bir yaklaşım, SLA'ların daha iyi anlaşılmasını, yönetilmesini ve SLA'larda tanımlanmış olan her bir denetimin gerçek zamanlı ya da yarı gerçek zamanlı olarak bulut sistemlerine entegrasyonunu sağlamaktadır.

Bulut servisleri ve bulut güvenliği üzerine yapılan SLA ontolojileri ile ilgili çalışmaların araştırılması ve incelenmesi, bu konuda yapılacak olan gelecekteki çalışmaların kapsamını belirleyecek ve geliştirilecek ontolojilerin hedeflerini net biçimde tanımlayacaktır. Araştırma ve inceleme çalışması, alanın daha iyi anlaşılmasını ve daha etkili güvenlik çözümleri geliştirilmesini sağlar.

Bu çalışmada, bulut servisleri ve bulut güvenliği için SLA ontolojileri oluşturulması üzerine kapsamlı bir araştırma ve inceleme yapılmıştır. Çalışmanın 2. bölümünde yapılan incelemenin yöntemi, araştırma soruları, arama stratejisi ve dahil etme/çıkarma kriterlerinin seçilmesi sağlanmıştır. 3. bölümde literatür incelemesi ile ilgili bulgulara yer verilmiştir. Çalışmanın son bölümü olan 4. bölümünde ise sonuçlar ve çıkarımlar eklenmiş, araştırma sorularına cevapların bulunabilirliği belirlenmiş, konu ile ilgili literatürdeki eksiklikler ve gelecekte yapılabilecek çalışmalar özetlenmiştir.

2. Yöntem

Çalışmada, bulut servisleri ve bulut güvenliği için SLA ontolojileri oluşturulması üzerine kapsamlı bir araştırma ve inceleme sunulmuştur. İnceleme kapsamında, Şekil 1'de gösterilmiş olan sistematik literatür taraması prosedürleri takip edilmiş (Kitchenham, 2004), yazılım mühendisliği alanında yapılması planlanan literatür incelemesi çalışmalarındaki kapsama uyulmuştur (Brereton ve ark., 2007). Bu prosedürler ve kapsam kullanılarak, literatürün tarafsız ve sistematik bir şekilde incelenmesi sağlanmıştır.



Şekil 1. Takip edilen yöntem özeti.

2.1. Araştırma Sorularını Belirleme

Literatürdeki çalışmaları kapsamlı şekilde tanımlama amacı ile, konu ile ilgili aşağıdaki 5 araştırma sorusu belirlenmiştir:

- AS1:Bulut servisleri ve bulut güvenliği SLA'ları için mevcut ontolojiler nelerdir ve hangi kavramları, ilişkileri kapsamaktadır?
- AS2:Bulut servisleri için SLA ontolojileri nasıl oluşturulur?
- AS3:Bulut servisleri için SLA ontolojileri, SLA uyumsuzluklarını belirlemede nasıl bir rol oynar?
- AS4:Bulut güvenliği için SLA ontolojileri, güvenlik

tabanlı SLA uyumsuzluklarını belirlemede nasıl bir rol oynar?

- AS5:Mevcut bulut servisleri ve bulut güvenliği SLA ontolojilerinin sınırlamaları nelerdir ve bu sınırlamaları aşmak için getirilmiş çözümler nelerdir?

Bu araştırma soruları kapsamında gerçekleştirilen sistematik literatür incelemesi, 2 ana başlık altında incelenmiş, elde edilen çalışmalarla ilgili tüm detaylar bu 2 başlık altında toplanmıştır:

- Bulut servisleri için SLA ontolojileri oluşturulması üzerine çalışmalar (AS1, AS2, AS3, AS5)
- Bulut güvenliği için SLA ontolojileri oluşturulması üzerine çalışmalar (AS1, AS4, AS5)

2.2. Arama Kriterlerini Belirleme

Bu çalışmada incelemede kullanılan kaynaklar, Google Scholar, Scopus, IEEE Xplore, ACM, Springer ve ResearchGate gibi elektronik bilgi ortamlarından elde edilmiştir. Seçilmiş olan elektronik bilgi ortamları, konuya dair tüm güncel ve tarafsız literatür çalışmalarını ve detaylarını içerdiğinden tercih edilmiştir. Literatür tarama ve inceleme çalışmalarının tamamı iki aylık süre içerisinde gerçekleştirilmiştir.

Araştırma sorularının belirlenmesinden sonra, bu araştırma sorularına cevap bulunacak şekilde, elektronik bilgi ortamları üzerinde yapılacak olan aramalarda temel olarak "Cloud", "Cloud Computing", "Cloud Security", "SLA" ve "Security", "Ontology" kelimeleri seçilmiştir. Bu kelimeler ek olarak, araştırma kapsamında faydalı sonuçlar elde edilebilecek olan "Cloud Services Computing", "Service Level Agreement", "Security Based Service Level Agreement", "Cloud Services", "Cyber Security", "Cloud Computing Security" terimleri de aramalara eklenmiştir. Bu aramaları yapabilmek için gerekli olan IEEE Xplore'a ait sorgu örnekleri Tablo 1'de gösterilmiştir. Sorgu örneklerindeki mantıksal yapıya uygun olacak şekilde diğer elektronik bilgi ortamlarında da benzer sorgular kullanılmıştır.

IEEE Xplore, ACM, ResearchGate üzerinde ilgili sorgular kullanılarak yapılan araştırmalardan elde edilmiş çalışmaların toplam sayıları Tablo 2'de belirtilmiştir. Google Scholar ve ResearchGate'ten gelen sayıların çok fazla ilgisiz çalışma içermesi ve Google Scholar'ın diğer kaynakların çalışmalarını da sayı olarak üzerinde barındırması gibi durumlar düşünüldüğünde karışıklık yaratmaması için belirtilmiş olan tabloda çalışma sayılarına yer verilmemiştir. Tabloda bu sayıların eklenmemesine karşılık, sistematik literatür çalışması kapsamında elektronik bilgi kaynağı olarak kullanılmıştır. Elde edilen çalışmalar, kitap bölümü, makale, konferans bildirisi gibi türlerin tamamını içermektedir.

Tablo 1. Literatür aramalarında kullanılan örnek sorgular

İlgili Çalışmalar	Sorgu Örnekleri
Bulut Servisleri ve SLA Ontoloji Odaklı Arama	("All Metadata":Cloud Computing) AND ("All Metadata":Service Level Agreement) OR ("All Metadata":SLA) AND ("All Metadata":Ontology)
Bulut Güvenliği ve SLA Ontolojisi Odaklı Arama	("All Metadata":Cloud Computing) AND ("All Metadata":Service Level Agreement) OR ("All Metadata":SLA) AND ("All Metadata":Ontology) AND ("All Metadata":Security) AND ("All Metadata":Cloud Security)

Tablo 2. Elde edilen çalışmaların toplam sayısı

Bilgi Ortamı	Bulut Servisleri ve SLA Ontoloji Odaklı Arama	Bulut Güvenliği ve SLA Ontolojisi Odaklı Arama	Yayın Yılları Aralığı
IEEE Xplore	37	9	2010-2023
ACM	165	137	1980-2023
Scopus	69	13	2003-2023
Springer	318	236	2000-2023
Toplam	589	395	-

2.3. Dahil Etme ve Çıkarma Kriterlerinin Belirlenmesi

Yapılmış olan çalışmaların sayısı oldukça çok gibi gözükse de çoğu araştırma soruları ile değerlendirilip filtrelendiğinde kapsam dışı kalmaktadır. Springer ve ACM üzerindeki çalışmaların çoğunun hem eski tarihli hem de konu ile ilişkisiz olduğu görülmüştür. Bu çıkarma kriterine ek olarak, aşağıdaki kriterlere göre yapılacak literatür incelemesinde kullanılacak olan çalışmalar belirlenmiştir:

- Seçilmiş olan çalışmaların yazım dili İngilizce olmalıdır.
- Seçilmiş olan çalışmalar 2013 yılı ve sonrasını kapsamalıdır. Zaman aralığı olarak son 10 yıl içerisinde yapılan çalışmalar belirlenmiştir. Bu kapsam, bulut bilişim teknolojisinin gelişmekte ve yenilenmekte olan bir teknoloji olması sebebi düşünülerek oluşturulmuştur.
- Kapsam açık şekilde tanımlanmış olmalı, kapsam dışı ya da daha geniş kapsamlı çalışmalar literatür incelemesine dahil edilmemelidir. Daha önceden belirlenmiş olan bulut servisleri için SLA ontolojileri

oluşturulması üzerine çalışmalar ve bulut güvenliği için SLA ontolojileri oluşturulması üzerine çalışmalar başlıklarını karşılar nitelikte olmalıdır.

2.4. Çalışmaların Seçilmesi

Belirtilmiş olan dahil etme ve çıkarma kriterleri kullanılarak seçilen çalışmalar, kullandıkları yöntemler ve uygulamalar, elde ettikleri sonuçlar ve gelecekte yapılması düşünülen çalışmalar gibi bakış açıları ile değerlendirilmiş ve bu literatür incelemesinde sunulmuştur. Çalışmaların seçilmesinde, dahil etme ve çıkarma kriterlerinin yanı sıra, içerik olarak yalnızca bulut servisleri ve bulut güvenliği odaklı SLA ontolojisi çalışmaları değerlendirilmiştir. SLA ontolojilerinin oluşturulmadığı ve literatüre herhangi bir yenilik getirmemiş olan çalışmalar, sistematik literatür inceleme kapsamından çıkartılmıştır. Belirlenen çalışmalar bulut servisleri ya da bulut güvenliği odaklı olmak üzere 2 ayrı kategoriye ayrılmıştır. Toplamda kriterlere uygun 10 çalışma belirlenmiştir. Bu çalışmaların listesi Tablo 3'te görülmektedir.

Tablo 3. Seçilen çalışmaların adı, kategorisi ve yayın yılı

Çalışmanın Adı	Kategori	Yayın Yılı
* An SLA Ontology to Support Service Discovery in Future Cloud Markets (Modica ve ark., 2013)	Bulut Servisleri, SLA ve Ontoloji	2013
* Automating Cloud Service Level Agreements using Semantic Technologies (Joshi ve Pearce , 2015)	Bulut Servisleri, SLA ve Ontoloji	2015
* Ontology of Secure Service Level Agreement (Lee ve ark., 2015a)	Bulut Güvenliği, SLA ve Ontoloji	2015
* Optimus: A Framework of Vulnerabilities, Attacks, Defenses and SLA Ontologies (Lee ve ark., 2015b)	Bulut Güvenliği, SLA ve Ontoloji	2015
* Automatic Extraction of Metrics from SLAs for Cloud Service Management (Mittal ve ark., 2016)	Bulut Servisleri, SLA ve Ontoloji	2016
* CSLAOnto: A Comprehensive Ontological SLA Model in Cloud Computing (Labidi ve ark.,2016)	Bulut Servisleri, SLA ve Ontoloji	2016
* Cloud SLA Modeling and Monitoring (Labidi ve ark., 2017a)	Bulut Servisleri, SLA ve Ontoloji	2017
* Ontology-Based SLA Negotiation and re-Negotiation for Cloud Computing (Labidi ve ark., 2017b)	Bulut Servisleri, SLA ve Ontoloji	2017
* Cloud SLA Terms Analysis Based On Ontology (Labidi ve ark., 2018)	Bulut Servisleri, SLA ve Ontoloji	2018
* A Semantically Rich Framework to Automate	Bulut Servisleri , SLA ve Ontoloji	2022

3. Bulgular

Bu kısımda, bulut servisleri ve bulut güvenliği için SLA ontolojisi oluşturulması üzerine çalışmalar ve elde edilen bulgular belirtilmiştir.

3.1. Bulut Servisleri için SLA Ontolojileri Oluşturulması Üzerine Çalışmalar

2013 yılında yapılmış olan bulut hizmeti sağlayıcılarının arz ve talep eşleştirmesini desteklemek için anlamsal ontoloji çerçevesi geliştirildiği bu çalışmada (Modica ve ark., 2013), bulut servisleri için SLA ontolojisi geliştirme alanlarına 3 farklı perspektiften bakılmıştır: Bulut sağlayıcısına özgü ontolojiler, bulut kullanıcılarına özgü ontolojiler ve her iki tarafın da kullandığı paylaşılan ontolojiler. Geliştirilen ontoloji "Practical Guide to Cloud Service Level Agreements" (Meegan ve ark., 2012) belgesi örnek alınarak oluşturulmuştur. Bu belge, bulut sağlayıcıları ile bulut kullanıcıları arasındaki deneyimleri birleştirmeyi amaçlar. Çalışma kapsamında, çerçevenin bir prototipi uygulanmış ve test edilmiştir. Uygulama ve test süreçlerinde Pellet teknolojisi (Pellet, 2023) kullanılmıştır. Amazon (AWS SLA, 2023), Rackspace (Rackspace SLA, 2023), GoGrid (GoGrid, 2023) SLA'ları kapsama dahil edilmiştir. Çalışmada 2 ayrı senaryo oluşturulmuş ve bunların analizleri gerçekleştirilmiştir. İlk senaryoda, bulut hizmetleri kullanıcısı bir hizmet olarak altyapı (*Infrastructure as a Service, IaaS*) servisini (Manvi ve Shyam, 2014) herhangi bir ücret ödemeden kullanmak istedikleri talebini iletir. Bu talep için oluşturulmuş olan ontoloji ve anlamsal çıkarım kuralına göre benzerlik oranı %100 olan servis ismi elde edilmiştir. Bunun yanı sıra, benzerlik oranı daha az olan servislerin çıkarımları da yapılmıştır. İkinci senaryoda ise, bulut hizmetleri kullanıcısı bir veri tabanı ve 3 özelliği SLA kapsamında tanımlanmış bir bulut servisi istenmiştir. Ontolojik çıkarım için, servis olarak yazılım (*Software as a Service, SaaS*) (WeiTek ve ark., 2014), uygulama için database, SLA parametreleri için ise ServiceAvailability, Confidentiality ve DataIntegrity belirlenmiştir. Geliştirilmiş olan ontoloji ve eklenen anlamsal ağ (*semantic web*) kurallarının sonucunda, veri tabanı servisi teklifi olarak oluşturulmuş servis çıktılarının benzerlik oranı en yüksek olanların AmazonRDSReservation ve MSAzureSQLFlat olduğu görülmüştür. Bu iki senaryodan yapılan çıkarımların sonuçları değerlendirildiğinde, geliştirilmiş ontolojinin ve anlamsal ağ kurallarının başarılı olduğu görülmektedir. Çalışmanın gelecek hedefleri olarak, bulut sağlayıcıları ve bulut hizmetleri kullanıcılarına ontolojik yapıya uygun talep ve teklifler oluşturmak için yarı otomatik uygulamalar sağlanacağı belirtilmiştir. Bu

uygulamalar sayesinde talep ve teklifler oluşturulması kolaylaşacaktır.

2015 yılında yapılmış olan diğer bir çalışmanın temel amacı (Joshi ve Pearce, 2015) bulut hizmetleri sağlayıcıları ve kullanıcıları arasında SLA kapsamında olan kontrolleri otomatize hale getirmektir. Bulut bilişim günden güne popüler hale geldikçe SLA kapsamındaki metrikleri ve kontrolleri manuel şekilde kontrol etmek zorlaşmış, aynı zamanda vakit kaybı haline gelmiştir. Bu sorunu çözmek için geliştirilmiş olan SLA tabanlı ontolojide, bulut sağlayıcılarının SLA ontolojilerini daha zengin bir şekilde tanımlayabildiklerinden anlamsal ağ teknolojisini (*Web Ontology Language, OWL*) kullanmışlardır. Terimler arasındaki ilişkileri ontolojiye eklerken yaşanan temel zorluk, belirli ölçülerin farklı bulut sağlayıcılarında farklı kelimelerle belirtilmiş olmasıdır. Örneğin "availability" kelimesi, başka bir bulut sağlayıcısında "uptime" olarak belirtilmiştir. Bütün bu kapsamlar ve ilişkiler geliştirilmiş olan ontolojiye eklenmiştir. Bunun yanı sıra, bulut sağlayıcılarının SLA kapsamları güncellenip yenilenebilir. Bu güncellemelerin göz önünde bulundurulması için SLA'da yapılan değişikliklerin yeni bir kaynak tanımlama çerçevesi (Resource Description Framework, RDF) grafiği olarak saklanması gerektiğini savunmuşlardır. Bu sayede, herhangi bir bulut hizmeti için bütün SLA kayıtlarına sahip olunabilecek ve SLA takibini ve kullanım planlamasını kolaylaştıracaktır. Çalışmada, yalnızca 4 bulut sağlayıcısının belirli servisler için olan SLA'ları kullanılmıştır. Bunlar, Google for Google Apps (Google SLA., 2023), Microsoft for MS Azure (Azure SLA., 2023) , Amazon EC2 (Amazon Compute SLA., 2023) ve Hewlett-Packard (HP SLA., 2023) olarak listelenmiştir. Çalışma ile ilgili gelecekte yapılacak aşamalar olarak, SLA'lara ek olarak gizlilik politikası belgeleri gibi bulut sağlayıcıları tarafından uygulanan gizlilik önlemleri ve denetimlerinin otomasyonu ve ontoloji çıkarımı ile ilgili çalışma yapılması hedeflenmektedir.

2016 yılında yapılmış olan çalışmada ise (Mittal ve ark., 2016), bulut tabanlı servisleri SLA'lar ile yönetmenin en kritik aşamalarından birinin SLA'ları sistemlerin anlayabileceği şekle dönüştürmek olduğundan bahsedilmiştir. SLA'ları sistemlerin anlayabileceği şekle dönüştürerek otomasyon ve düzenli izleme gibi konseptler bulut hizmetleri üzerinde uygulanabilmektedir. Bu motivasyondan yola çıkılarak çalışma kapsamında yazılım metinlerden oluşan SLA'lar üzerinde metin madenciliği (*text mining*) ve ontoloji geliştirmesi yapılmıştır. Bu geliştirmenin çıkarım yapan modülünde (*extractor*), SLA tanımlamaları, ilgili metriklerin, performans ölçütlerinin çıkarımı için desen tabanlı kurallar (*pattern based rules*) kullanılmıştır. Bu kurallar Stanford Pos Tagger (Stanford Pos Tagger, 2023) ve CMU Link Parser (Sleator ve Temperley, 1995). Çalışmanın değerlendirme (*assessor*) modülünde ise, bulut odaklı SLA ontolojisi oluşturulmuştur. SLA ontolojisinde, temel sınıflar bütün bulut uygulamalarında ortak olan özelliklerden oluşmaktadır. Örnek olarak hizmet sağlama, hizmet kullanılabilirliği, veri silinmesi gibi başlıklar düşünülebilir. Çalışmada ontoloji kapsamında RDF, SPARQL gibi anlamsal ağ teknolojileri kullanılmıştır. Çalışma kapsamında, gelecekte yapılacak eklentiler olarak, farklı bulut sağlayıcılarının SLA'ları kullanılarak karşılaştırma ve farklılıkları belirleme yapılması planlanmaktadır. Ayrıca SLA dışında diğer legal belgeler, zorunluluklar ve sözleşmelerden çıkarım yapılması ve ontolojik yapılara dönüştürülmesi amaçlanmaktadır.

2016 yılında geliştirilmiş olan CSLAOnto adlı çerçeve, (Labidi ve ark., 2016), Methontology (Fernández ve ark., 1997) rehber alınarak oluşturulmuştur. Methontology, ontoloji geliştirme süreçlerini yönetmek ve düzenlemek için tasarlanmış bir metodoloji çerçevesi olarak tanımlanır. Bu çerçeveye göre oluşturulacak olan CSLAOnto 4 ana başlıktan oluşmaktadır. İlk başlık olan tanımlama (*spesification*), ontolojinin anlamsal yapısından faydalanılarak SLA'nın temeldeki yapısını iyileştirme hem sistemler hem de bulut sağlayıcıları için anlaşılabilir ve okunabilir bir model elde etmeyi içerir. Ek olarak, ontolojinin çıkarım yeteneklerinden ve çıkarım kurallarının gücünden faydalanılarak SLA ihlallerini otomatik olarak tespit etmeyi amaçlamışlardır. İkinci başlık olan kavramsallaştırma (*conceptualization*) aşamasında, ontoloji kapsamındaki kavramlar tanımlanmıştır. SLA kapsamları incelendiğinde kavramlar 3 ayrı gruba bölünmüştür. Bu gruplar, bağlam, taraflar ve şartlar olarak listelenmiştir. Resmileştirme (*formalization*) bölümünde, anlamsal ağ teknolojileri ve Protégé (Gennaria J. ve ark., 2003) uygulaması kullanılarak ontoloji oluşturulma tamamlanmıştır. Son başlık olan doğrulama (*validation*) aşamasında ise, ontolojinin otomatik olarak ihlalleri belirlemesi için izleme (*monitoring*) kuralları tanımlanması amaçlanmıştır. Ardından, SLA belgesi örneklerinde bu kurallar uygulanmıştır. Çalışma içerisinde daha önceden geliştirilmiş diğer ontolojilerle belirli parametreler üzerinden karşılaştırılmış bir tablo bulunmaktadır. Bu tabloya göre, CSLAOnto, genel olarak yapılmış diğer çalışmalardan daha geniş bir kapsam içerir. Buna ek olarak hizmet ve dağıtım bulutu modellerinin tamamını kapsayacak şekilde geliştirilmiştir. Gelecekte yapılacak olan detaylar kapsamında, geliştirdikleri ontolojinin esnekliğinden faydalanarak bulut üzerindeki servislerin SLA kapsamına uymaması durumunda otomatik düzeltme entegrasyonu yapılması planlanmaktadır.

2017 yılında yapılmış olan bir diğer çalışmada (Labidi ve ark., 2017a) ilk olarak SLA tabanlı izlemenin zorluklarından ve yapılan çalışmanın motivasyonlarından bahsedilmiştir. Her bir bulut sağlayıcısı farklı SLA belgelerine ve farklı izleme politikalarına sahiptir. Bu farklılıklar, belirli kontrollerin ve tanımların farklı şekilde temsil edilmesine yol açmaktadır. Aynı amaçla yazılmış olan bu SLA kontrollerini ve izleme yöntemlerini otomatize etmek, bu farklı temsil etme biçimlerinden dolayı zorlaşmaktadır. Farklı bulut sağlayıcılarının farklı şekilde tanımlanmış ve

yazılmış olan SLA'larına ek olarak, aynı bulut sağlayıcılarının farklı servisleri için tanımlanmış SLA'larda farklılıklar olabilmektedir. Bulut servislerinin yapıları farklıdır, bu sebeple servislerin farklı parametreleri ve farklı hesaplama biçimleri olacaktır. Bu şekildeki farklılıklar, SLA tabanlı izleme ve ihlallerle ilgili aksiyon almanın otomatikleştirilmesini zorlaştırır. Yapılmış olan çalışmada bu sorunları çözmek için ontoloji yapısının kullanılmasının gerekli olduğu vurgulanmaktadır. Ontoloji gerekliliği, 2 sebebe dayanır. Bunlardan ilki, ontoloji kullanıldığında SLA'ların daha okunabilir ve anlaşılabilir olmasıdır. Bir diğer sebep, kurulabilecek ontolojik bir yapıda bilgi çıkarımları (*knowledge extraction*) sayesinde, SLA ihlalleri ve bildirme gibi operasyonlar otomatize şekilde oluşturulmaktadır. Bu sebeplerden yola çıkılarak, bulut SLA'ları kullanılarak ontoloji geliştirme ve ihlal durumlarını otomatik bildirme ve aksiyon alma çerçevesi tasarlanmıştır. Yaklaşım, 2 aşamalıdır. İlk aşamada, CSLAMOnto (Labidi ve ark., 2017a) çerçevesi, SLA dokümanlarını ontolojik bir yapıya dönüştürür. Bu dönüşümde OWL teknolojisi kullanılmıştır. Yaklaşımın ikinci aşamasında, oluşturulmuş olan SLA ontolojisi, SLA ihlallerini otomatize şekilde bildirmek için kullanılır. Bunun yapılabilmesi için Anlamsal Ağ Kural Dili (*Semantic Web Rule Language, SWRL*) kullanılmıştır. Yazılacak olan kurallara göre, ihlaller tespit edilip, gerekli aksiyonlar alınır. Yapılmış olan çalışmanın devamında, uygulanabilirliğini kanıtlamak amacı ile uygulanabilirlik kanıtlama (*Proof of Concept, PoC*) gerçekleştirilmiştir. Bu PoC'da, CSLA2M adıyla geliştirilmiş olan çerçeve kullanılmıştır. Bu çerçeve, farklı bulut sağlayıcılarının SLA'larını destekler. Bulut sağlayıcısı kullanıcısı tarafında aktifleştirilmesi gereken bu çerçeve, SLA ihlallerini bildirmeye yöneliktir. Çerçevenin kullanılmasında, ilk olarak SLA'nın seçimi sağlanır. Sonrasında, SLA modelinin ontolojisi çerçeve üzerinden oluşturulur. Son olarak SLA'ya bağlı olarak izleme ve ihlal aşaması başlatılır. Burada, erişilebilirlik, hata oranı gibi belirli metriklerin izlenmesi sağlanır. Metriklerle ilgili verilerin toplanması ve çerçeveye gönderilmesi için PoC aşamasında CloudSim çerçevesi kullanılmıştır. CloudSim, bulut bilişim ortamlarını modellemek ve simüle etmek için tasarlanmış bir çerçevedir (CloudSim, 2023). Eklenen SWRL kuralları ile, geliştirilen çerçeve çeşitli hizmetlerin neden olduğu birden çok SLA ihlalinin verimli bir şekilde tespit edilmesini sağlamıştır. Son olarak, konu ile ilgili bir vaka analizi (*case study*) çalışması yapılmıştır. Bu analiz, geliştirilmiş olan SLA ontoloji modelleri ile karşılaştırma amaçlı gerçekleştirilmiştir. Yapılan çalışmada, Amazon EC2, S3 ve Microsoft Azure SLA'ları kullanılmış, rSLA (Mohamed ve ark., 2017) , CSLA (Kouki ve ark., 2012) ,SLAM (Moustafa ve ark., 2015), CSLAMOnto (Labidi T. ve ark., 2017a) ve Ontology-Base Service Monitoring (Dastjerdi ve ark., 2012) çalışmaları karşılaştırılmıştır. Yapılmış olan analizde ilk kriterde, SLA ontoloji modellerini oluşturmak ve kuralları yazmak için geçen süre karşılaştırılmış ve CSLAMOnto'nun SLA ontolojiyi en kısa sürede oluşturduğu görülmüştür. Ardından, ontoloji kuralları kapsamında, CSLAMOnto'da 20 kural yazılmışken, diğerlerinde ortalama olarak 34 kurala ihtiyaç duyulduğu tespit edilmiştir. Daha fazla kurala ihtiyaç duyulması, diğer ontolojik sistemlerin daha karmaşık bir yapıda olduğunu kanıtlar. Vaka analizinde karşılaştırılan ikinci kriter ise, ihlal tespitindeki başarı oranlarını (*accuracy rate*) karşılaştırmaktır. Bu karşılaştırma sonucunda geliştirilen çerçevenin duyarlılık (*recall*) değerinin %80, kesinlik (*precision*) değerinin %88 olduğu görülmüştür. Duyarlılık ve kesinlik değerleri, diğer çalışmalardan daha fazladır.

Diğer bir çalışmada (Labidi ve ark., 2017b), bulut sağlayıcıları ve bulut kullanıcılarının SLA üzerinde anlaşmasını sağlamak için ontoloji tabanlı müzakere (*negotiation*) ve yeniden müzakere (*re-Negotitation*) yöntemi sunulmuştur. Yönteme dair çalışmalar gerçekleştirilirken, OWL ve SWRL teknolojileri kullanılmıştır. İlk olarak, modelleme aşamasında, bulut sağlayıcıları ve kullanıcıları iki ayrı ontoloji oluşturur. Eşleme (*mapping*) aşamasında, oluşturulmuş olan iki ontoloji arasında eşleştirme yapılır. İki tarafın arasındaki eşlenme sağlandığında, ontoloji oluşturulur. Ontoloji oluşturulma modeli ayrıca Cloud SLA Ontology (Labidi ve ark.,2016) çalışmasında da açıklanmıştır. Ontoloji oluşturulduktan sonra, bulut hizmetlerinde değişiklik algılandığında model otomatik olarak tetiklenmiştir. İlk olarak, SLA detaylarını etkileyebilecek parametreleri içeren bulut hizmeti ontolojisi tanımlanmıştır. Ardından, bulut hizmeti bağlamsal değişiklikleri hakkında akıl yürütme ve gerekirse SLA detaylarını sisteme için çıkarım kuralları oluşturulmuştur.

Geliştirilmiş olan SLA ontolojisi (Labidi ve ark., 2018) ile SLA'nın daha anlaşılabilir olmasını amaçlayan Labidi ve arkadaşları, müşteri isteklerine ve farklılıklarına göre akıl yürütme (*reasoning*) teknikleri kullanarak özelleştirmeyi de hedeflemişlerdir. Bunlara ek olarak, SLA terimlerinden yeni bilgi çıkarımları ile SLA ontoloji analiz süreçlerini iyileştirme, çalışmanın motivasyonları arasındadır. Geliştirilmiş olan ontoloji "Cloud SLA Analyzing Ontology" olarak isimlendirilmiştir. Kısaltması "CSLA2Onto" şeklindedir. Yapılmış olan SLA analizlerinde, SWRL kuralları oluşturularak çıkarımlar yapılması sağlanmıştır. Bu kurallar, zaman içerisinde yaşanabilecek SLA ya da bulut servisleri tabanlı değişikliklere uyum sağlayabilmek ve haberdar olabilmek için oluşturulmuştur. Analiz kısmında toplamda 3 farklı analiz türü belirtilmiştir. İlk model olan dinamik fiyatlandırma modelinde, verilecek olan fiyatlandırma modeli parametresine göre servislere ait fiyatlandırmanın hesaplanması ile ilgili kural eklenmiştir. Fiyatlandırma modelleri "PayAsYouGo", "PayForResource", "Subscription" olarak belirlenmiştir. Her bir model için özel olarak hesaplama kuralları tanımlanmıştır. Geliştirilen ikinci modelde bulut servisleri ile toplam ihlal ve ceza sayıları ile ilgili kural eklenmiştir. Son model olan otomatik SLA sonlandırma

ile ilgili modelde ise SLA'ya uymayan durumlar belirlendiğinde, SLA iptali, SLA sonlanması, kural ihlallerine göre güncelleme isteme gibi durumları otomatize şekilde belirleme amacıyla kural seti oluşturulmuştur. CSLA2Onto'ya ek olarak, "Cloud SLA Analyzing" diğer bir adıyla CSL2A prototipi geliştirilmiştir. Bu geliştirme, SLA analizini otomatikleştirmeyi bir adım öteye taşımayı hedeflemektedir. SLA ayrıştırma, ontolojinin yapısını zenginleştirme ve analiz modülleri bulunmaktadır. Çalışma kapsamında, gelecekte yapılacak olan çalışma olarak, SLA ihlalini otomatik olarak tahmin edip bu tahmine bağlı olarak yönetim süreci oluşturmak hedeflenmektedir.

Anlamsal ağ teknolojileri kullanılarak 2022 yılında yayınlanmış SLA ontoloji çerçevesinde (Ganapathy D. ve Josh K., 2022) , SLA üzerindeki terimler ve aralarındaki ilişkisel yapı oluşturulurken NIST standartlarıyla (NIST, 2023) eşleşecek şekilde geliştirilmiştir. NIST standartlarından, sınıflar ve bahsedilmiş olan terimler arasındaki ilişkisel yapılar temel alınmıştır. Geliştirilmiş olan çerçevede metodoloji şu şekildedir: İlk olarak farklı bulut sağlayıcılarının sahip olduğu farklı SLA'lar kullanılarak metin madenciliği yöntemiyle farklı bileşenlerin çıkarılması sağlanır. Bu bileşenler ontolojik yapı için sınıf, alt sınıf ve ilişkiler olarak tanımlanır. Bu çerçeve kullanılarak farklı sorgular ile farklı kullanıcı ihtiyaçlarına karşılık gelen en uygun bulut servis sağlayıcısı belirlenir. Bu çalışmada eğitim aşaması için kullanılan veri setleri, VMWare Cloud Air (VMWare Cloud Air., 2023) , Amazon Web Services (AWS SLA, 2023), Azure (Azure SLA, 2023), GCP (Google SLA., 2023), IBM Softlayer (IBM SLA, 2023) SLA dokümanları olarak listelenmiştir. Test için ise RackSpace (Rackspace SLA, 2023), SAP (SAP SLA, 2023) , Alibaba (Alibaba SLA, 2023) ve Oracle SLA'ları (Oracle SLA, 2023) kullanılmıştır. Veri setlerinden metin çıkarımı aşamalarında CMU Link Parser ve düzenli ifade (*regular expression*) entegrasyonları yapılmıştır. Çalışma kapsamında oluşturulmuş olan SLA ontoloji çerçevesinin sonuçlarının doğrulanması için katılımcı değerlendirmesi (*actor evaluation*) çalışmasında, ontoloji çıkarımlarının doğruluğunu kontrol etmek için anket çalışması yapılmıştır. Bu anket çalışmasına göre bulut SLA tabanlı 10 tane durum belirlenmiş ve geliştirilen ontolojinin çıkardığı sonuçlar ve çoğunluğun cevapları karşılaştırılmıştır. Bu anket çalışmasının temel amacı, insanların SLA dokümanlarından anlamlandırma ve SLA ontolojisinin yaptığı anlamsal çıkarımları karşılaştırmaktır. Karşılaştırma sonunda %90'lık başarı oranı olduğu görülmüştür. Yalnızca 1 durumda uyumsuzluk olduğu saptanmıştır. Bunun sebebi, durumun karmaşıklığıdır ve ontoloji çerçevesi kapsamında beklenen bir davranıştır. Çalışma kapsamında daha karmaşık bir kural eklenerek bu sorunun üstesinden gelinebileceğini belirtmişlerdir. Gelecekte yapılacak çalışmalar olarak, SLA dokümanlarına ek olarak bulut tabanlı uyumluluk, bulut servisleri kapsamı ve sorumluluk sigortası gibi raporların ontoloji kapsamına eklenmesi planlanmaktadır. Buna ek olarak, daha karmaşık durumlara karşılık ontolojilerin anlamsal çıkarımlarının doğruluğunu arttırma hedeflenmektedir. Yapılmak istenen bu çalışmalarda, veri setlerinin arttırılması da amaçlanmaktadır.

Bulut güvenliği için SLA ontolojileri oluşturulması üzerine çalışmalar

Bulut sistemleri üzerinde güvenlik ve gizlilik (*privacy*) prensiplerini uygulamanın zor olduğu ve bulut tabanlı uygulamaların üzerindeki zafiyet sayısı arttıkça yönetimin de zor hale geldiğini vurgulayan bu çalışmada (Lee ve ark., 2015a), güvenlik tabanlı SLA ontolojisi geliştirilmiş ve SSLA olarak kısaltılmıştır. SSLA ontolojisi ile, güvenlik SLA'ları daha kolay anlaşılabilmekte, bulut hizmeti kullanıcıları ontolojileri karşılaştırarak kullanacağı bulut sağlayıcısına karar verebilmekte ve SLA tabanlı güvenlik izleme hizmetleri daha kolay hale gelmektedir. Bu avantajlar, ontoloji yapısının makine tarafından okunabilir (*machine readable*) ve kolayca entegre edilebilir olmasından kaynaklanmaktadır. Avantajlara ek olarak, geliştirilen çerçeve SSLA'nın uyumluluklar (*compliance*) için belirli düzenlemeleri karşılayıp karşılamadığını belirlemek için bir yöntem sağlar. Çalışmanın tartışma bölümü iki temel başlık altında incelenmiştir:

- Taraflara faydaları: Bulut altyapı sağlayıcısı tarafından bakıldığında, garanti edilen güvenlik düzeylerini sunmak ve sunulduğundan emin olmak için geliştirilen çerçeveyi kullanarak geliştirme yapabilir. Bulut servis sağlayıcısı tarafından bakıldığında ise, sağlanılan hizmetlerle ilgili uyumluluk sorunlarını anlamak için geliştirilen çerçeveyi kullanabilir.
- Veri ihlali (*Data Breach*): Bir veri ihlali meydana geldiğinde, geliştirilmiş olan çerçeveye göre atak yüzeyi ve atağın getirebileceği olası zarar tespiti yapılabilir.

Gelecekte yapılacak çalışmalar olarak, geliştirilen çerçeveye dayalı WS-Anlaşması (*WS-Agreement*) tabanlı WSAG4J5'te SLA'yı SSLA'ya genişletmeyi planlamışlardır. WS-Agreement, SLA oluşturmak ve yönetmek için kullanılır (WSAG4J, 2023). Yapılacak bu geliştirme ile güvenlik tabanlı SLA yönetimi ve izlemesi gibi aksiyonlar otomatikleştirilecektir.

2015 yılında yapılmış diğer bir çalışma, (Lee ve ark., 2015b), "Ontology of Secure Service Level Agreement" çalışması geliştirilerek oluşturulmuştur. Geliştirilmiş olan Optimus çerçevesi, iki bölümden oluşmaktadır: Güvenlik tabanlı SLA ontolojisi ve güvenlik değerlendirmesi (*security assessment*). Güvenlik tabanlı SLA ontolojisi, bulut bilişimin güvenlik alanlarını kapsayan genelleştirilmiş SLA'lar kullanılarak modellenmiştir. Güvenlik değerlendirmesi, güvenlik tabanlı SLA ontolojisinin genişletilerek güvenlik açıkları, saldırılar ve savunma yöntemleri detaylarının eklenmesiyle ontoloji bilgi tabanları (*ontology knowledge bases – OKB*) oluşturulmak amacı ile geliştirilmiştir. Geliştirilen

güvenlik tabanlı SLA ontolojisinde toplam 13 sınıf (*class*) oluşturulmuştur. Bu sınıflardan bazılarının isimleri ve açıklamaları aşağıda belirtilmiştir:

- Networking (Ağ): Ağ yapıları ile ilgili tanımlanan sınıftır. TrafficIsolation, IndividualBandwidth, IPAddressQuantity alt sınıflarına sahiptir.
- Vulnerability (Zafiyet): Bilinen güvenlik açıklarını tespit etme ve çözümleri tanımlar.
- CryptoSpec (Kriptografik Spesifikasyonlar): Bulut sistemleri üzerindeki kriptografik geliştirmelerle ilgili olan sınıftır.
- AccessControl (Erişim Denetimi): Bu sınıf, erişim kimlik doğrulamasını, yetkilendirmeyi, mobil erişim şemaları ve kurallarını tanımlar.
- Compliance (Uyumluluk): Bulut hizmetlerinin, yasaların gerektirdiği şekilde güvenlik ve gizlilik standartları ve uygulamalarıyla uyumlu olduğu onaylanmalıdır. Bu sınıfın ontoloji içinde yer alması gerekliliktir.

Geliştirilen güvenlik değerlendirmesi ise, National Vulnerability Database (NVD), Common Vulnerability Scoring System (CVSS) metrikleri gibi detayların geliştirilmiş SLA ontolojisine eklenmesi ile oluşturulmuştur. Bu sayede güvenlik bilgi tabanları anlamsal olarak modellenmiştir. Güvenlik detaylarının anlamsal yapısı, her bir modeli nasıl temsil etmek istediğimize ve modellerin birbirleriyle nasıl etkileşime girdiğine ilişkin tanımlı verileri eklememize izin verir. Gelecekte yapılacak çalışmalar olarak, ontoloji ve güvenlik değerlendirmesi tabanlı farklı seviyelerde güvenlik yapılandırmalarına sahip bulut hizmetleri sunmak amacıyla uygulama geliştirileceğini öngörmüştür.

4. Sonuç

Bu çalışmada bulut servisleri ve bulut güvenliği için SLA ontolojileri oluşturulması üzerine sistematik literatür incelemesi yapılmıştır. İlk olarak, yöntem, araştırma soruları, arama stratejisi ve dahil etme ve çıkarma kriterleri belirlenmiş, bu filtrelemelerin sonucunda toplamda 10 farklı çalışma inceleme kapsamına dahil edilmiştir. Çalışmalar seçilirken kapsamı ve araştırılan terimleri tam olarak karşılamasına özellikle dikkat edilmiştir. İnceleme kapsamında çıkarılan sonuçlar aşağıda özetlenmiştir:

- Bulut servisleri için SLA ontolojisi geliştirilme üzerine çalışmaların sayısının, bulut güvenliği için SLA ontolojisi geliştirilme çalışmalarının sayısından fazla olduğu görülmüştür. Gelecek çalışmalar olarak, bulut güvenliği ontolojilerine odaklanılması bu çalışma kapsamında önerilmektedir.
- Seçilen çalışmaların geneline bakıldığında, belirli kişilerin bu konularda çalışma yaptığı dikkat çekmektedir. Bulut servisleri ve bulut güvenliği üzerine geliştirilecek SLA ontolojilerinin faydaları düşünüldüğünde, bulut servisleri ya da bulut güvenliği tabanlı teknolojilerle ilgili çalışma yapılacaksa, SLA ontolojisi kapsamına odaklanılabilir.
- Seçilen çalışmaların tamamında, belirli bulut sağlayıcılarının SLA'ları üzerinden yola çıkılmış, bunlara odaklı ontolojiler oluşturulmuştur. Günümüzde, bulut servislerinin kullanılabilirliği, maliyet analizi, dayanıklılığı gibi SLA parametreleri, bulut servislerinin sağladığı servisler tarafından kontrol edilebilmektedir. SLA ontolojisi tarafında eksik olan, bulut servislerini kullanarak uygulama geliştiren şirketlerin kendi SLA'larından ontoloji geliştirme ve güvenlik süreçlerine dahil etme ve otomatikleştirme süreçleridir. Daha önceden yapılmış çalışmalarda belirli bulut sağlayıcılarından yapılan çıkarımlarla oluşturulan ontolojilerin, özelleştirilmiş ve yapı olarak birbirinden farklı olabilecek diğer SLA yapılarını karşılayamayacağı öngörülmektedir. Bu sebeple, gelecek çalışma olarak, herhangi bir SLA dokümanı için otomatikleştirilmiş ontolojik çıkarım çalışmaları ve bunların bulut üzerinde çalışan uygulamaların süreçlerine dahil edilmesi düşünülebilir.

Yapılmış olan literatür çalışmasında, bulut servisleri ve bulut güvenliğine odaklı SLA ontolojileri ile ilgili güncel çalışmalar incelenmiş ve bir bütün olarak sunulmuştur. Daha önceden yapılmış olan çalışmalar incelendiğinde, bu konu ile ilgili bir literatür çalışması bulunmadığı görülmüştür. Bu çalışma ile birlikte, bulut servisleri ve bulut güvenliği tabanlı SLA ontolojilerinin literatürdeki yeri ve gelecekte yapılabilecek olan çalışmalar ile ilgili genel bir çerçeve oluşmuştur. Çalışmanın kapsamı SLA ontolojileri ile sınırlıdır, SLA'ların metin belgeleri olarak düzenlendiği düşünüldüğünde, metinler üzerinde uygulanabilecek doğal dil işleme uygulamalarının SLA'lar ile kullanımı ilgili literatür çalışmaları gelecekte yapılacak olan çalışmalardan biri olarak düşünülebilir.

Katkı Oranı Beyanı

Yazar(lar)ın katkı yüzdesi aşağıda verilmiştir. Tüm yazarlar makaleyi incelemiş ve onaylamıştır.

	S.Y	Ö.C
K	70	30
T	70	30
Y	70	30
VTI	70	30
VAY	70	30
KT	70	30
YZ	80	20
KI	40	60
GR	40	60

K= kavram, T= tasarım, Y= yönetim, VTI= veri toplama ve/veya işleme, VAY= veri analizi ve/veya yorumlama, KT= kaynak tarama, YZ= Yazım, KI= kritik inceleme, GR= gönderim ve revizyon.

Çatışma Beyanı

Yazarlar bu çalışmada hiçbir çıkar ilişkisi olmadığını beyan etmektedirler.

Kaynaklar

Alibaba SLA. 2023. Alibaba service level agreements. URL: https://www.alibabacloud.com/help/en/legal/latest/product-sla. (accessed date: 23 March, 2023).

Amazon Web Services (AWS) SLA. 2023. AWS service level agreements (SLAs). URL: https://aws.amazon.com/legal/service-level-agreements. (accessed date: 23 March, 2023).

Amazon Compute SLA. 2023. Amazon compute service level agreement. URL: https://aws.amazon.com/compute/sla/. (accessed date: 23 March, 2023).

Avram MG. 2014. Advantages and challenges of adopting cloud computing from an enterprise perspective. Procedia Technol, 12: 529-534

Azure SLA. 2023. Azure Service Level Agreements. URL: https://www.azure.cn/en-us/support/legal/sla/. (accessed date: 23 March, 2023).

Baset S. 2012. Cloud SLAs: present and future. ACM SIGOPS Operating Systems Rev, 46: 57–66.

Brereton P, Kitchenham A, Budgen D, Turner M, Khalil M. 2007. Lessons from applying the systematic literature review process within the software engineering domain. Journal of Systems and Software. Volume 80, 571-583.

CloudSim. 2023. A framework for modeling and simulation of cloud computing infrastructures and services. URL: https://github.com/Cloudslab/cloudsim. (accessed date: 23 March, 2023).

Dastjerdi A, Tabatabaei S, Buyya R. 2012. A dependency-aware ontology-based approach for deploying service level agreement monitoring services in cloud. Softw Pract Exper, 42(4): 501–518.

Fernández M, Gómez-Pérez A, Juristo N. 1997. Methontology: From ontological art towards ontological engineering. AAAI Technical Report, 1997: 33-40

Ganapathy D, Josh K. 2022. A semantically rich framework to automate cloud service level agreements. IEEE Transactions on Services Computing, 2022: 1-12.

Gennaria J, Musen M, Fergerson R, Grosso W, Crubezy M, Eriksson H, Noy N, Tu S, 2003, The evolution of Protégé: an environment for knowledge-based systems development, Inter J Human-Computer Stud, 58(1): 89-123.

Google SLA. 2023. Google cloud platform service level agreements. URL: https://cloud.google.com/terms/sla (accessed date: 23 March, 2023).

GoGrid. 2023. What is GoGrid? URL: https://en.wikipedia.org/wiki/GoGrid (accessed date: 23 March, 2023).

HP SLA. 2023. HP support service agreement terms & conditions. https://h20345.www2.hp.com/Resources/csndocs/elfpack/AU_EN/Related%20Documents/Terms_and_conditions.pdf (accessed date: 23 March, 2023).

IBM SLA. 2023. IBM service level agreements. URL: https://cloud.ibm.com/docs/overview?topic=overview-slas (accessed date: 23 March, 2023).

Joshi K, Pearce C. 2015. Automating cloud service level agreements using semantic technologies. Proceedings of IEEE International Conference on Cloud Engineering (IC2E), March 9-13 2015, Tempe, AZ, USA, pp: 1-6.

Kitchenham B. 2004. Procedures for performing systematic reviews. Keele University, Technical Report, TR/SE-0401, Newcastle, UK, ISSN:1353-7776, pp: 33.

Kouki Y, Ledoux T. 2012. CSLA: A language for improving cloud SLA management. international conference on cloud computing and services science. URL: https://www.scitepress.org/papers/2012/39564/39564.pdf (accessed date: 23 March, 2023).

Labidi T, Mtibaa A, Brabra H. 2016. CSLAOnto: A comprehensive ontological sla model in cloud computing. J Data Semant, 5: 179–193.

Labidi T, Mtibaa A, Gaaloul W, Tata S, Gargouri F. 2017a. Cloud SLA modeling and monitoring. Proceedings of IEEE 14th International Conference on Services Computing, June 25-30, 2017, Honolulu, Hawaii, USA, pp: 338-345. DOI: 10.1109/SCC.2017.50

Labidi T, Mtibaa A, Gaaloul W, Gargouri F. 2017b. Ontology-Based SLA negotiation and re-negotiation for cloud computing. Proceedings of IEEE 26th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, 21-23 June, 2017, Tempe, AZ, USA, pp: 36-41. DOI: 10.1109/WETICE.2017.24

Labidi T, Mtibaa A, Gargouri F. 2018. Cloud SLA terms analysis based on ontology. Procedia Comput Sci, 126: 292-301.

Lee C, Kavi K, Raymond P, Gomathisankaran M. 2015a. Ontology of secure service level agreement. Proceedings of 16th International Symposium on High Assurance Systems Engineering, January 8-10, 2015, Daytona, USA, pp: 166-172. DOI: 10.1109/HASE.2015.33

Lee C, Kamongi P, Kav K. 2015b. Optimus: A framework of vulnerabilities, attacks, defenses and SLA ontologies. Inter J Next-Generation Comput, 6(1): 42-56.

Manvi S, Shyam G, 2014, Resource Management for Infrastructure as a Service (IaaS) in cloud computing: A survey. J Network Comput Applicat, 41: 424-440.

Meegan J, Singh. G, Woodward, S, Salvatore V, Rak M, Harris D, Murray G, Martino B Di, Roux Le, McDonald J, Kean R, Edwards M, Russell D, Malekkos G, 2012, Practical guide to cloud service level agreements. URL: https://parsec2.unicampania.it/venticinque/index.php/research/jr-project?view=publication&task=show&id=149 (accessed date: 03 June, 2023).

Mittal S, Joshi K, Pearce C, Joshi A. 2016. Automatic extraction of metrics from slas for cloud service management. Proceedings of IEEE International Conference on Cloud Engineering (IC2E), April 4-8, 2016, Berlin, Germany, pp: 1-4. DOI: 10.1109/IC2E.2016.14

Modica G, Petralia G, Tomarchio O. 2013. An SLA ontology to support service discovery in future cloud markets. Proceedings of 27th International Conference on Advanced Information Networking and Applications Workshops, March 25-28, 2013, Barcelona, Spain, pp: 1-5. DOI: 10.1109/WAINA.2013.68

Mohamed M, Anya O, Tata S, Mandagere N, Baracaldo N, Ludwig H. 2017. rSLA: An Approach for Managing Service Level Agreements in Cloud Environments. Inter J Cooperat Inform Systems, 26(2): 1742003. DOI: 10.1142/S0218843017420035

Moustafa S, Elgazzar K, Martin P, Elsayed M. 2015. SLAM: SLA monitoring framework for federated cloud services. Proceedings of IEEE/ACM 8th International Conference on Utility and Cloud Computing, December 7-10, 2015, Limassol, Cyprus pp: 1-6. DOI: 10.1109/UCC.2015.90

NIST. NIST ontological visualization interface for standards: user's guide. URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7945.pdf /(accessed date: June 03, 2023).

Ontology. 2023. What is Ontology? URL: https://en.wikipedia.org/wiki/Ontology (accessed date: 23 March, 2023).

Oracle SLA. 2023. Oracle cloud infrastructure service level agreement (SLA). URL:

https://www.oracle.com/uk/cloud/sla/(accessed date: 23 March, 2023).

SAP SLA. 2023. SAP service level agreement. URL: https://help.sap.com/docs/HANA_SERVICE/319dbc7c518f4f31b7333060d0cc546c/9deb7aea417a4e1886d7845e198fc9b5.html (accessed date: 23 March, 2023).

Singh A, Chatterjee K, 2017. Cloud security issues and challenges: A survey, J Network Comput Applicat, 79: 88-115.

Sleator D, Temperley D. 1995. Parsing English with a link grammar. URL: https://arxiv.org/pdf/cmp-lg/9508004.pdf (accessed date: 23 March, 2023).

Stanford PoS Tagger. 2023. The Stanford POS Tagger. URL: http://www.linguisticsweb.org/doku.php?id=linguisticsweb:tutorials:automaticannotation:stanford_pos_tagger (accessed date: 23 March, 2023).

Pellet. 2023. What is pellet? URL: https://www.w3.org/2001/sw/wiki/Pellet (accessed date: 23 March, 2023).

Rackspace SLA. 2023. Rackspace service level agreements. URL: https://docs.rackspace.com/docs/vm-management/private-cloud/service-level-agreements (accessed date: 23 March, 2023).

VMWare Cloud Air. 2023. VMware vCloud air service description. URL: https://www.vmware.com/files/au/pdf/vcloud-air/vcloud-air-Datasheet.pdf (accessed date: 23 March, 2023).

WeiTek T, XiaoYing BAI, Yu H. 2014. Software-as-a-service (SaaS): perspectives and challenges. Sci China Inform Sci, 57: 1-15.

WSAG4J. 2023. Welcome to WSAG4J. https://wsag4j.sourceforge.net/site/index.html. (accessed date: 23 March, 2023).