Web Servislerde Meydana Gelen Plansız Kesintilerin Tespiti

***

Detection Of Unplanned Interruptions Occurring in Web Services

Erkan MERAL[1]
Sami ACAR[2]

DOI:10.33461/uybisbbd.1000007

Makale Bilgileri

Makale Türü: Araştırma Makalesi

Geliş Tarihi: 23.09.2021

Kabul Tarihi: 26.12.2021

Öz

Kamu kurumları görevlerini ifa ederken diğer kamu kurumlarının verilerine ihtiyaç duymaktadır. İhtiyaç duyulan bu veriler, kamu kurumlarının birçok iş sürecini web uygulamaları aracılığıyla gerçekleştirmeleriyle birlikte günümüzde web servisler kullanılarak anlık olarak temin edilmektedir. Web servislerle alınan veriler, kamu kurumlarının kritik iş süreçlerinde de kullanılabilmektedir. Kritik iş süreçlerini gerçekleştiren bilgisayar uygulamaları için kesinti tolerasyon süresi çok kısa olabilmektedir. Bu tip uygulamalar için donanım arızası veya ağda gerçekleşen bağlantı kopmaları gibi aksaklıklar nedeniyle web servislerde meydana gelen kesintilerin tespit edilme süresi önemli bir konudur. Bu çalışma ile kamu kurumları arasında veri paylaşımında kullanılan web servisler için kesintilerin yönetimine yönelik bir yönetim modeli sunulmaktadır. Söz konusu yönetim modeli ile kamu kurumları web servislerini birbirleri ile doğrudan paylaşmayacak, Merkezi Web Servis Yönetim Sistemi adı verilen merkezileştirilmiş bir yazılım aracılığıyla paylaşacaklardır. Bu yazılıma entegre edilen tüm web servisler için Windows servisler geliştirilecek ve bu Windows servisler kullanılarak belirli periyotlarda otomatik olarak ilgili web servislerden sorgular gerçekleştirilecek ve bu sorgular sayesinde kesintiler tespit edilecektir. Windows servis sorgularının çalışma zaman aralıklarına göre, web servislerde meydana gelen kesintilerin ortalama olarak ne kadar sürede tespit edileceği çalışma sonunda verilmiştir.

***Anahtar Kelimeler**: web servis, veri paylaşımı, web servislerde kesinti, kesinti yönetimi, Windows servis.*

Abstract

Public institutions need the data of other public institutions while performing their duties. This needed data is provided instantaneously by using web services today, together with the fact that public institutions carry out many business processes through web applications. Data received via web services can also be used in critical business processes of public institutions. For computer applications that perform critical business processes, the interruption tolerance time can be very short. For this type of applications detection time of interruptions in web services due to hardware failures or network disconnections is an important issue. In this study, a management model for the management of interruptions for web services used in data sharing between public institutions is presented. With this management model, public institutions will not share web services directly with each other, but will share them through a centralized software called the Central Web Service Management System. Windows services will be developed for all web services integrated into this software, and queries will be made from related web services automatically at certain periods by using these Windows services, and interruptions will be detected thanks to these queries. At the end of the study, the average duration of the interruptions in web services according to the operating time intervals of Windows service queries is given.

***Keywords:** web service, data sharing, web services interruption, interruption management, Windows service.*

Article Info

Paper Type: Research Paper

Received: 23.09.2021

Accepted: 26.12.2021

Atıf/ to Cite (APA): Meral, E. ve Acar, S. (2021). Web Servislerde Meydana Gelen Plansız Kesintilerin Tespiti. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 5(2), 212-225

[1] Gazi Üniversitesi, Bilişim Enstitüsü, Bilişim Sistemleri Bölümü, erkan.meral@outlook.com, Ankara, Türkiye,
[2] Dr. Öğr. Üyesi, Gazi Üniversitesi, Uygulamalı Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, samiacar@gazi.edu.tr

1. GİRİŞ

Kamu kurumları görevlerini yerine getirebilmesi için kendi bünyesinde barındırdığı verilerin yanı sıra diğer kamu kurumlarının verilerine de ihtiyaç duyabilmektedir. İhtiyaç duyduğu bu verileri statik olarak CD, DVD vb. araçlarla diğer kamu kurumlarından temin edebilmekteyken, kurumların iş süreçlerini bilgisayar uygulamalarıyla gerçekleştirmesiyle birlikte veriler kurumlar arasında internet ortamında anlık olarak dinamik şekilde de paylaşılabilmektedir. Farklı kurumların sahip oldukları uygulamaların birbirine anlık veri aktarımı günümüzde web servis teknolojisi ile mümkün olabilmektedir (Balıkcı, 2014). Web servisler, internet üzerinde web uygulamalarının entegrasyonu için yeni ve çekici bir yaklaşım olarak görülmekte (Benharref vd., 2010) olup web servislerin ana odağı dağıtılmış ve heterojen uygulamalar arasında birlikte çalışabilirliği sağlamaktır (Oh vd., 2008). Web servisler, yayımlanabilen ve standart web protokolleri ile ağ üzerinden erişilebilen platform bağımsız ve özerk hesaplama birimleri olarak tanımlanmakta ve kamu kurumları arasında kullanımının yanı sıra iş dünyasında da dağıtık uygulama geliştirme standardı olarak kabul görmektedirler (Gümüş ve Yürek, 2015). Kamu kurumları arasında ihtiyaç duyulan verilerin çevrimiçi olarak aktarılması konusu kurumların iş süreçlerinin gerçekleştirilmesinde ciddi oranda fayda sağlamaktadır. Web servislerin diğer kurumlarla paylaşılması için internet ortamında yayımlanması belirli kolaylıklar getirirken, birçok güvenlik tehdidini de beraberinde getirmektedir. Web ortamı güvensizdir ve internet ortamındaki her bilgisayar uygulaması güvenlik tehditleriyle karşı karşıyadır (Oliveira vd., 2020).

Literatür taraması sonucunda, yapılan çalışmalar incelendiğinde, birçok çalışmada web servis ile veri paylaşım işlemlerinin güvenli bir zemine oturtulması üzerine odaklanıldığı görülmüştür. Bir çalışmada (Sarıkoz, 2015), web hizmetlerini siber güvenlik saldırılarından korumak için ağ tabanlı güvenlik, protokol tabanlı güvenlik, imza tabanlı güvenlik ve diğer denetim mekanizmaları gibi farklı bakış açıları açısından çeşitli çalışmalar yapılması gerekliliğinden bahsedilmiş ve bir kurumsal ağın bir web hizmetinin tüm güvenlik yönlerini tanımlamak için bir bilgi güvenliği çerçevesi önerilmiştir. Bu çerçevede, çeşitli saldırı türlerine ilişkin olarak bir web hizmeti için örnek bir bilgi güvenliği modellemesi sunulmuştur. Sözü edilen modelleme, önceden tanımlanmış ve belirlenmiş senaryolar için test edilmiş ve ölçülmüştür. Bir çalışmada (Yue ve Tao, 2012) da farklı sistemler arasında kullanılan web servislerdeki Microsoft .NET ve Apache Axis platformlarının birbirleriyle haberleşebildiği bir güvenlik modeli önerilmiştir. Başka bir çalışmada (Deniz, 2009), güvenlik fonksiyonlarının web servisleri olarak sunulduğu ve tanımlı olan web servislerini güvenli hale getirmeyi hedefleyen bir alt yapı teknoloji modelinin sunulması amaçlanmış ve alt yapı teknolojisinin prensipleri ve mimari modeli sunulmuştur. Önerilen alt yapı teknoloji modeli ile kimlik doğrulama, yetki belirleme, denetim izlerinin (log) tutulması, istisna-hata yönetimi ve raporlama gibi güvenlik fonksiyonları web servisleri olarak modellenmiştir. Diğer bir çalışmada (Bacı, 2008), güvenli iletişimde önemle üzerinde durulan .NET platformu kullanılarak geliştirilen web servisleri kavramı incelenmiş ve yapılan örnek olay incelemesi, istemcinin statüsünün geçerliliğini denetlemek için web servisince sağlanan kimlik belirteci kullanılmış olup kod bazlı yapılarca uygulanan RIJNDAEL, 3DES ve RSA algoritmaları kullanılarak, web servisleri ve onların istemcileri arasında güvenli iletişim sağlamayı ispatlamada kullanılmıştır. Bu algoritmaların işlevselliğini elde etmek için iletişim boyunca farklı kriptografik algoritmalar ve ağ ortamları kullanılarak bu algoritmaların operasyon değerlerinin belirlenmesi için testler yapılmıştır. Bir çalışmada (Sarıman ve Küçüksille, 2016) ise web servis uygulamalarının tek bir test modeline göre değerlendirilmesiyle muhtemel açıklıkların yeterince tespit edilemeyeceğinden bahsedilmiş, web servislerinin güvenliğini test etmek için geliştirilen hibrit model sunulmuştur. Söz konusu hibrit modelde güvenlik testleri sırasında kullanılan statik ve dinamik analizin yanında gözden geçirme yöntemi dâhil edilerek, otomatize araçların bulamadığı açıklıklar tespit edilebileceği değerlendirilmiştir. Web servisler üzerinde gerçekleştirilen güvenlik çalışmaları, web servislerin çalıştırılmalarında performans sorunlarına neden olabilmektedir. Yapılan bir çalışmada (Bakırov, 2012), web servislerin güvenliğinin sağlanması adına oluşturulan güvenlik politikalarının birçok zorlukları giderdiği ancak bunların performans konusunda kayda değer ek yükleri beraberinde getirdiğinden bahsedilmiştir. Çalışmada Temel Kimlik

Doğrulaması, Digest uygulanan Kimlik Doğrulaması, Kerberos Kimlik Doğrulaması ve SSL Güvenlik tekniklerini SOAP-tabanlı ve RESTful web servisleri üzerinde gerçekleştirerek ilgili güvenlik önlemlerinin performansa etkisi araştırılmıştır. Sonuç olarak, RESTful web servislerinin SOAP tabanlı web servislerine kıyasla daha iyi sonuçlar verdiği saptanmıştır. Bu sonucun RESTful web servislerinin daha az ek yük getirmesi ile yakından ilgili olduğu değerlendirilmiştir. Ayrıca, test sonuçlarına göre Kerberos Kimlik Doğrulama tekniği diğer tekniklere kıyasla performans konusunda çok daha fazla ek yük getirdiği ortaya konulmuştur.

Son dönemlerde Türkiye'de web servisler ile veri paylaşımı konusunda yetkili otoriteler tarafından da web servislerin kullanımı hususunda birçok çalışma yapılmıştır. Web servislerle veri alışverişinin bir standarda oturtulmasını sağlayan, 28 Şubat 2009 tarih ve 27155 sayılı Kamu Bilgi Sistemlerinde Birlikte Çalışabilirlik Esasları konulu Başbakanlık Genelgesi ile yürürlüğe konulan Birlikte Çalışabilirlik Esasları Rehberi (Devlet Planlama Teşkilatı, 2009) bu konuda yapılan önemli bir çalışmadır. Birlikte Çalışabilirlik Esasları Rehberi, e-Dönüşüm Türkiye Projesi kapsamında başta kamu kurum ve kuruluşları olmak üzere kamuya elektronik ortamda hizmet sunan tüm kurumlar arasında birlikte çalışabilirliği sağlamak ve bu çerçevede yetki, sorumluluk, esas, prensip, yöntem ve kriterler ile teknik standartları belirlemek amacıyla yayımlanmıştır. Kamu kaynaklarıyla yürütülen tüm bilgi ve iletişim teknolojileri yatırımlarında, bu Rehber'de belirtilen esas ve standartlara uyumun zorunlu olduğu belirtilmiştir. Önemli bir çalışma da kamu kurumları arasında veri alışverişlerinde kullanılan web servislerin internet ortamından değil de internet ortamından izole KamuNet (Kamu Sanal Ağı) adı verilen ağ üzerinden sağlanmasına yönelik KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ'dir (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2017). KamuNet, kamu kurum ve kuruluşları tarafından özel ağ ile internet ortamından yalıtılmış şekilde hizmet, işlem ve veri trafiğinin aktarılacağı, fiziksel ve siber saldırılara karşı daha güvenli kapalı devre kamu sanal ağı altyapısıdır. KamuNet, kamu kurum ve kuruluşları tarafından içerik güvenliği sağlanan veri iletişiminin, kurumlar arası internete kapalı olan daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun altyapının tesis edilmesi ve planlanan ortak veri merkezi/merkezlerinin dâhil edilmesi amacıyla oluşturulmuştur. Bir diğer çalışma, yine web servislerin karşı karşıya kalacağı tehditlere yönelik olarak Türk Standartları Enstitüsü tarafından yayımlanan Web Servis Güvenliği için Ortak Kriterler Koruma Profili'dir (Türk Standartları Enstitüsü, 2021).

Literatürde, bilgi sistemleri üzerinde gerçekleşen kesintilere yönelik çalışmaların da var olduğu görülmektedir. Yapılan bir çalışmada (Kutlugün, 2018), bilgi sistemlerinde meydana gelen kesintilerin sebeplerini tespit etmek amacıyla, kesintiye sebep olan olaylar Hata Ağacı Analizi yöntemi ile incelenmiş ve kesinti maliyetlerinin azaltılması ve performans iyileştirme üzerine çalışılmıştır. Çalışmada ayrıca, kesintiye neden olan problemlere göre alınması gereken önlemler ve kullanılan yöntemin geliştirilmesi için çözüm önerileri sunulmuştur. Bir çalışmada (Kalantari vd., 2020), web hizmetlerinde kesintileri azaltmak ve sistem erişilebilirliğini artırmak üzerine çalışılmıştır. Çalışmada önerilen yöntem ile web hizmetlerinde meydana gelen arıza oranının %30 azaltıldığı görülmüştür. Başka bir çalışmada (Gunawi vd., 2016) ise bulut hizmeti verilen sistemlerde 7 (yedi) yıl içerisinde meydana gelen 597 plansız kesinti için kesinti süreleri, kesintilerin temel nedenleri, etkileri ve kesintileri düzeltme prosedürleri analiz edilmiştir.

Literatürdeki çalışmalardan da görüldüğü üzere gerek kurumlar arası veri paylaşımına yönelik olarak yapılan çalışmalar, gerekse kamu otoriteleri tarafından yayımlanan Birlikte Çalışabilirlik Esasları Rehberi, KamuNet Tebliği ve Web Servis Güvenliği için Ortak Kriterler Koruma Profili çalışmaları ile web servislerle veri aktarımı konusunda sistemsel ve network ile ilgili güvenlik konuları, güvenlik çalışmaları sonucunda oluşan performans kayıpları ve kimlik doğrulama gibi birçok konu ele alınmıştır. Bunun yanı sıra bilgi sistemlerinde meydana gelen kesintilere yönelik olarak gerçekleştirilen çalışmalarda genellikle kesintilerin neden kaynaklandığına, kesintilerin meydana gelmemesi ya da azaltılması, kesintilerden en az etkilenilmesi ve kesintilerin giderilmesi için yapılması gereken çalışmalara odaklanılmış, ancak web servislerde meydana gelen kesintilerin

yönetilmesine (kesinti meydana geldiğinin tespit edilmesini sağlayacak mekanizmanın geliştirilmesi gibi konuların yönetimsel bir yaklaşım ile ele alınması) ve plansız kesintilerin tespit süresinin kısaltılmasına yönelik bir çalışma yapılmamıştır.

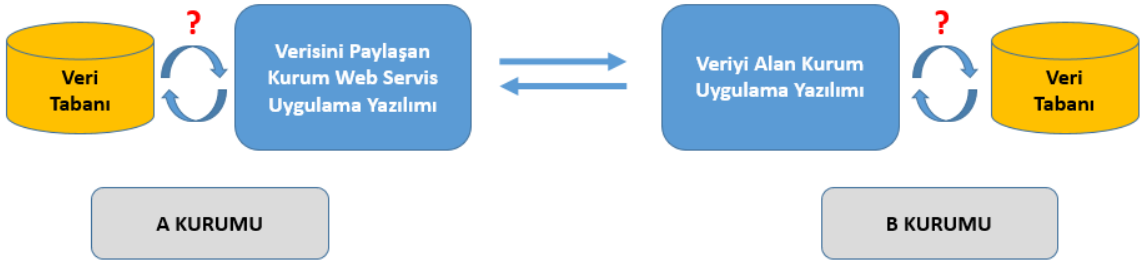
Bu çalışmada, kamu kurumları arasında veri paylaşımında kullanılan web servislerde meydana gelen plansız kesintilerin tespit edilmesi üzerine odaklanılmış ve plansız kesintilerin tespit sürelerinin kısaltılması için Windows servislerden yararlanılmıştır.

Bölüm 2'de Windows servislere ilişkin çalışma detayları özetlenmiştir. Bölüm 3'te uygulanan tekniğe ilişkin bulgulara yer verilmiştir. Son olarak Bölüm 4'te çalışma sonuçları verilmiştir.

2. WEB SERVİS KESİNTİLERİNİN TESPİT EDİLMESİ

Kamu kurumları kendisine ait verileri diğer kurumlar ile paylaşması gerektiği durumlarda ilgili verilere ait web servis uygulaması oluştururlar. Bu web servisleri daha önceleri internet ortamında yayıma alırken, KamuNet ağının oluşturulması ile bu ağ üzerinden yayıma almaya başlamışlardır. Veriyi talep eden Kurumlar, KamuNet üzerinde yayımlanan web servisleri kullanarak ihtiyacı olan verileri elde edebilmektedirler.

Şekil 1'de A Kurumunun verisini paylaşmak üzere oluşturduğu web servis uygulaması üzerinden B Kurumu uygulaması ile veri paylaşım mekanizması gösterilmektedir.



Şekil 1. Veri Paylaşım Mekanizması

Şekil 1'de görüldüğü üzere herhangi bir aracı olmadan kurumlar doğrudan verilerini birbirleriyle paylaşmaktadırlar. Aynı zamanda paylaşılan ve temin edilen verilere ilişkin denetim izlerinin tutulması A ve B Kurumlarının inisiyatifinde gerçekleşmektedir.

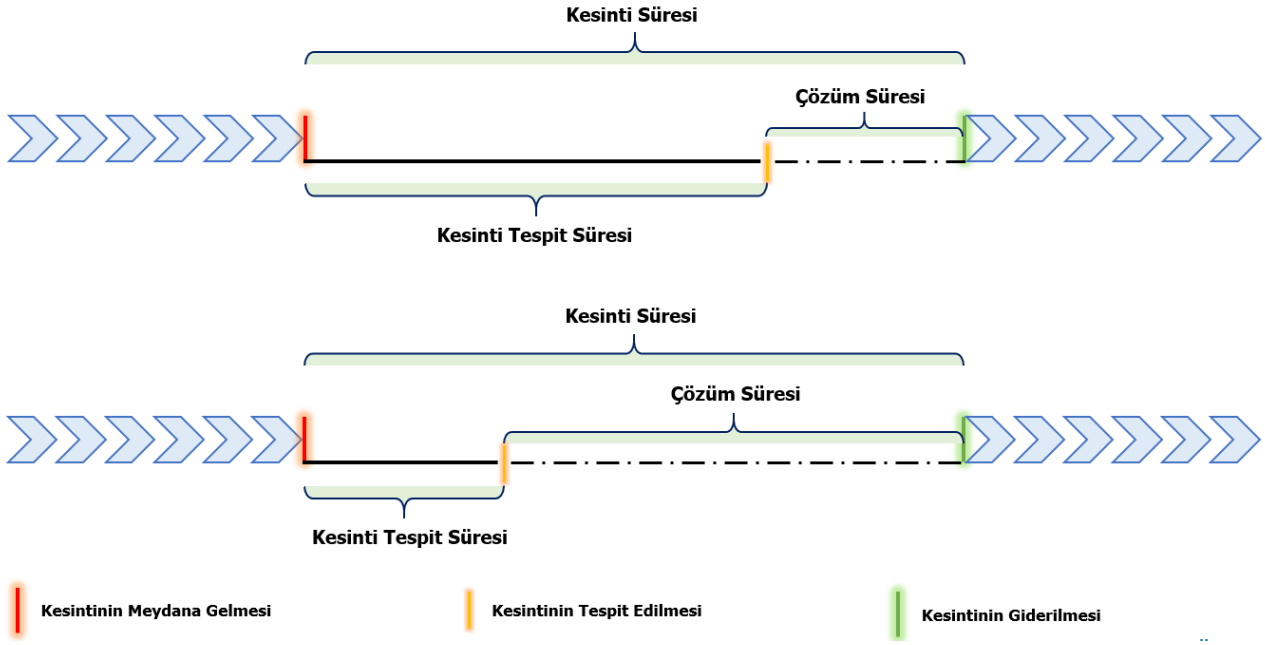
Kamu kurumları diğer kurumlara ait web servisleri kendi uygulamaları ile entegre ettiklerinde, kurum kullanıcıları diğer kurumlara ait verilere web uygulamaları üzerinden erişebilmektedirler. Ancak bu web servislerde bazı dönemlerde kesinti meydana gelebilmektedir (Kutlugün, 2018). Meydana gelen bu kesintiler planlı veya plansız olarak gerçekleşebilmektedir.

Planlı kesintiler, verisini paylaşan kurumların bilgisayar uygulamalarında gerçekleştirecekleri bakım, güncelleme vb. nedenlerle belirli zaman aralığında kontrollü bir şekilde yapılan kesintilerdir. Bu durumlarda veri paylaşımı yapan kurum, verisini paylaştığı kurumlara kesinti yapılacağına dair bilgi vermektedir. Planlı kesintilerde web servisin yaklaşık ne kadar süre hizmet dışı kalacağı belirlidir ve kesintinin meydana geldiği zaman kesin olarak bilinmektedir.

Plansız kesintiler, donanım arızası veya ağda gerçekleşen bağlantı kopmaları gibi aksaklıklar nedeniyle verisini paylaşan kurumun kontrolünde olmadan gerçekleşen kesintilerdir. Bu durumda kesintiden web servisi kullanan kullanıcılar haberdar olmadığı için servisler üzerinden sorgulama yapıldığında servisten veri gelmeyecektir. Böyle bir durum ile karşılaşıldığında web servis sahibi kurum ile iletişime geçilip sorun ile ilgili geri bildirim verilecektir. Kamu kurumları, sahibi oldukları

web servislerden veri çekilemediği durumlarda sistemin kendilerine haber vermesi için alarm mekanizmaları da oluşturabilmektedirler. Bu durumda servislerde beklenmeyen bir kesinti olması durumunda kullanıcılar tarafından gerçekleştirilen ilk sorgulama ile üretilen alarm sayesinde haberdar olabilmektedirler.

Şekil 2'de web servislerde meydana gelen kesintilerin sürelerinin hangi bileşenlerden oluştuğu gösterilmiştir. Bileşenlerden biri kesinti tespit süresi, diğeri ise kesinti nedeninin ortadan kaldırılması için geçen süre olan çözüm süresidir.



Şekil 2. Kesinti Süresi Bileşenleri

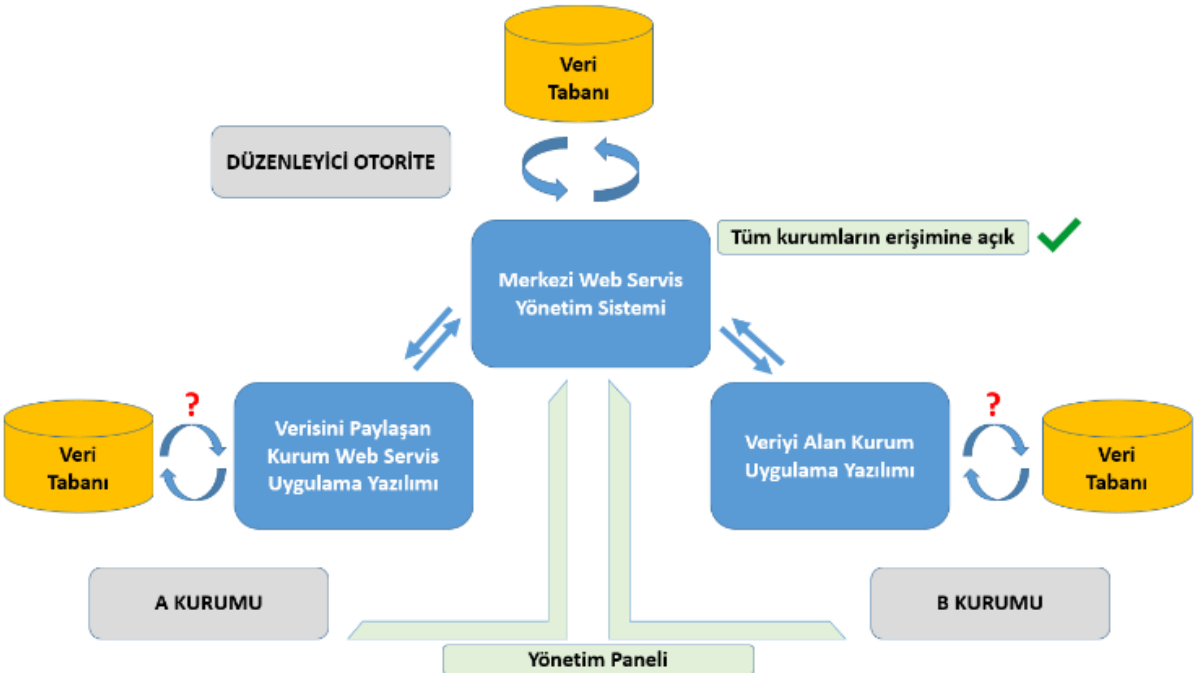
Planlı kesintilerde kesinti web servis sahibi kurum tarafından gerçekleştirildiği için kesinti tespit süresi sıfırdır ve kesinti süresi çözüm süresinden ibarettir. Plansız kesintilerde ise kesintinin tespit edilmesi için bir miktar süre geçeceği için Şekil 2'de gösterilen birinci ve ikinci durumdakine benzer şekilde bir kesinti süresi olacağından bahsedilebilir. Şekildeki birinci durumda kesintinin tespit edilme süresinin çözüm süresinden daha uzun olduğu görülmektedir. İkinci durumda ise çözüm süresinin tespit süresinden uzun olduğu görülmektedir.

Plansız kesintilerin tespitinde kullanıcılar tarafından gerçekleştirilen sorgulardan faydalanılabilir. Ancak kullanıcı sorgularının uzun zaman aralıklarında gerçekleşmesi durumunda kesintilerin tespit edilmesi uzun zaman alacaktır. Bu çalışmada, plansız kesintilerin tespit sürelerinin kısaltılması amaçlanmış ve kullanıcı sorgularının gerçekleşmesi beklenmeden plansız kesintilerin tespit edilebilmesini mümkün kılan Windows servisler kullanılmıştır.

Çalışmada Windows servisler belirli bir zaman aralığında otomatik olarak web servislerden sorgulama yapma üzerine programlanmakta, ilgili web servislerden veri gelmediği durumlarda alarmlar üretmekte ve kesinti kaydı oluşturmaktadırlar. Bu sayede hem plansız kesintiler konusunda ilgililere haber verilmekte hem de kesintinin ne zaman meydana geldiği ve ne zaman sona erdiği konusunda otomatik olarak kayıtlar oluşturulmaktadır.

Diğer kurumlara ait web servislerden veri çeken her kurum Windows servisler kullanarak web servislerden devrede olup olmadığını tespit etmek amacıyla belirli zaman aralıklarında veri çekerse, bir web servisin birçok kurum tarafından kullanılma durumunda ilgili web servis üzerinden birçok kurum Windows servis aracılığıyla çok sayıda veri çekmiş olacaktır. Bu durumun önüne geçilmesi

için çalışma kapsamında web servislerin tek bir uygulamaya entegre edilerek bu uygulama üzerinden verilerin dağıtılması değerlendirilmiştir. Çalışmada, web servislerin entegre edildiği bu uygulamaya Merkezi Web Servis Yönetim Sistemi (MWSY) adı verilmiştir. Bu durumda Kurumlar web servisler üzerinden veri çekme işlemlerinde, verisini paylaşan kurumun web servisine doğrudan erişim sağlamayacak, MWSY aracılığıyla dolaylı yoldan erişim sağlayacaktır. Çalışma kapsamında veri paylaşımına yönelik önerilen yönetim modeli (Yönetim Modeli) Şekil 3'te gösterilmiştir.



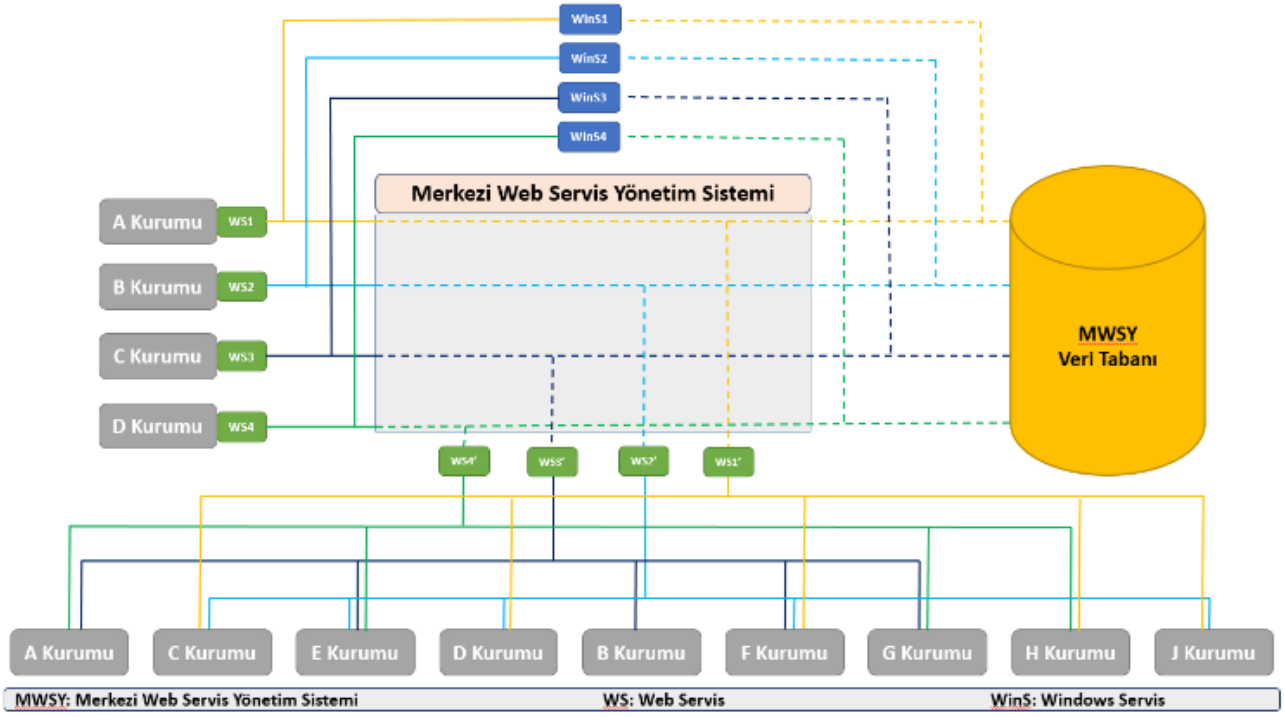
Şekil 3. Veri Paylaşımına Yönelik Önerilen Yönetim Modeli

Yönetim Modelinin sunulduğu Şekil 3'te görüldüğü üzere, A Kurumuna ait web servis MWSY yazılımına entegre edilmiş ve MWSY yazılımı üzerinden yeni bir web servis yayımlanmıştır. B Kurumuna ait uygulamalar da yeni yayımlanan bu web servise entegre edilmiştir. B Kurumu bu servis üzerinden veri çekeceğinde bu servis, A Kurumuna ait web servis üzerinden veriyi çekmekte ve B Kurumuna iletmektedir. Kısaca MWSY yazılımı veri alan kurumların web uygulamaları ile verisini paylaşan kurumların web servis uygulamaları arasında köprü görevi görmektedir. MWSY yazılımı düzenleyici bir otorite tarafından yönetilmektedir.

Yönetim Modelinde MWSY yazılımına entegre edilen tüm web servisler için ayrı ayrı Windows servisler oluşturulmaktadır. Bu Windows servisler belirli zaman aralıklarında otomatik olarak çalışmakta ve web servislerde plansız bir kesintinin meydana gelip gelmediğini tespit etmek amacıyla web servislerden sorgular gerçekleştirmektedirler. Windows servis üzerinden gerçekleştirilen sorgu, aynı web servise erişen bütün kurumlar için hizmet etmekte olup serviste kesinti meydana gelmiş ise verisini paylaşan kuruma ve web servisten veri çekmekte yetkili tüm kurumlara alarm gönderilmektedir. Bu sayede web servis sahibi kurumun kesintiden haberdar olması sağlanmakta ve web servisten veri çekmekte yetkili kurumların da serviste kesinti olduğu için servisten veri çekemeyeceği bilgisini edinmesi sağlanmaktadır. Yönetim Modeli ile her kurumun ayrı ayrı Windows servisler geliştirip plansız kesinti tespiti için sorgular çekmesinin önüne geçilmekte ve merkezileştirilmiş sistem sayesinde bir Windows servis sorgusu ile plansız kesintilerin tespit edilmesi sağlanmaktadır.

Yönetim Modeline ilişkin veri akış şeması Şekil 4'te verilmiştir. Şekilde gösterildiği gibi MWSY yazılımının kendisine ait verilerini kaydedeceği bir veri tabanı bulunmaktadır. Web servisler

üzerinden kullanıcılar tarafından manuel ve Windows servisler tarafından otomatik olarak gerçekleştirilen tüm sorgulara ilişkin kayıtlar bu veri tabanına kaydedilmektedir. Benzer şekilde yazılıma entegre edilen web servislerde meydana gelen planlı ve plansız kesintilerin kayıtları da bu veri tabanına kaydedilmektedir.



Şekil 4. Önerilen Yönetim Modeli Veri Akış Şeması

Çalışma kapsamında, Yönetim Modelinin uygulama ortamında gösterimi için bir simülasyon ortamı hazırlanmıştır. Simülasyon ortamı için MWSY yazılımı, bu yazılıma entegre 8 (sekiz) adet web servis ve bu web servislerden otomatik olarak veri çekmek için 8 (sekiz) adet Windows servis uygulamaları geliştirilmiştir. Geliştirilen tüm uygulamalar Asp.NET ve C# programlama dili kullanılarak geliştirilmiştir.

MWSY yazılımında Merkezi Yönetici ve Kurum Yetkilisi kullanıcı rolleri mevcuttur. Rollerine göre kullanıcılar aşağıdaki işlemleri gerçekleştirebilmektedir.

MWSY yazılımında Merkezi Yönetici rolü ile yapılabilecek işlemler:

- Sisteme entegre edilmiş tüm web servislere ilişkin bilgilerin görüntülenmesi,
- Sistemde kayıtlı olan bir web servisin geçici olarak hizmet dışı bırakılması (Bu durumda web servisin sahibi kurum ile web servisi kullanmakta yetkili olan tüm kurumlara planlı bir kesinti yapıldığına dair otomatik bildirim gönderilir.),
- Geçici olarak hizmet dışı bırakılan bir web servisin hizmete açılması (Bu durumda web servisin sahibi kurum ile web servisi kullanmakta yetkili olan tüm kurumlara planlı kesintinin sona erdirildiğine dair otomatik bildirim gönderilir.),
- Sisteme entegre edilmiş web servislerin sahibi kurumlar ile web servisleri kullanmakta yetkili olan kurum bilgilerinin görüntülenmesi,
- Sisteme entegre edilmiş tüm web servislerden sorgulama yapılması,
- Web servislerden gerçekleştirilen tüm kurumların sorgulama işlemlerine ilişkin bilgilerin görüntülenmesi,

- Web servislerde meydana gelen tüm planlı ve plansız kesintilere ilişkin bilgilerin görüntülenmesi,
- Sistemde kayıtlı kurumlara SMS ve E-mail şeklinde kesintiler ile ilgili bildirim yapılması ve gönderilen bildirimlerin görüntülenmesi.

MWSY yazılımında Kurum Yetkilisi rolü ile yapılabilecek işlemler:

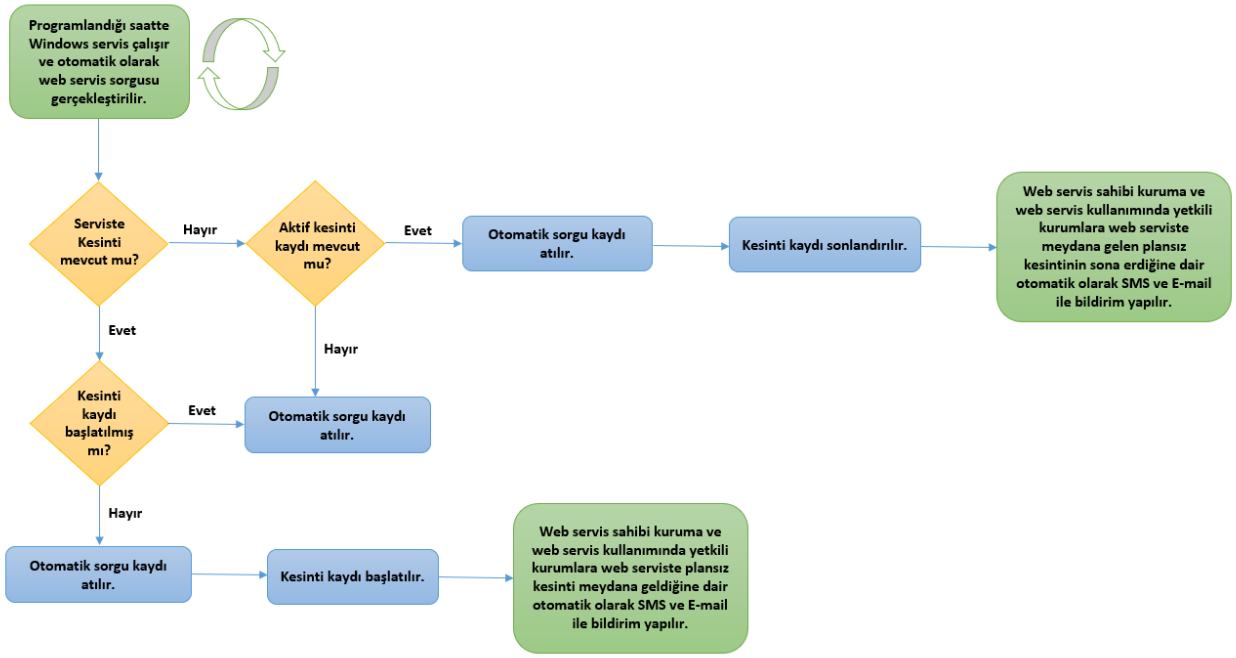
- Sisteme entegre edilmiş sahibi olunan web servislere ilişkin bilgilerin görüntülenmesi,
- Sistemde kayıtlı olan ve sahibi olunan bir web servisin geçici olarak hizmet dışı bırakılması (Bu durumda web servisi kullanmakta yetkili olan tüm kurumlara planlı bir kesinti yapıldığına dair otomatik bildirim gönderilir.),
- Sistemde kayıtlı olan ve sahibi olunan geçici olarak hizmet dışı bırakılan bir web servisin hizmete açılması (Bu durumda web servisi kullanmakta yetkili olan tüm kurumlara planlı kesintinin sona erdirildiğine dair otomatik bildirim gönderilir.),
- Sisteme entegre edilmiş sahibi olunan web servisleri kullanmakta yetkili olan kurum bilgilerinin görüntülenmesi,
- Sisteme entegre edilmiş kullanmakta yetkili olunan web servislerin bilgileri ile bu web servislerin sahipleri olan kurum bilgilerinin görüntülenmesi,
- Sisteme entegre edilmiş kullanmakta yetkili olunan web servislerden sorgulama yapılması,
- Sahibi olunan web servislerden gerçekleştirilen tüm kurumların sorgulama işlemlerine ilişkin bilgilerin görüntülenmesi,
- Kullanmakta yetkili olunan web servislerden tarafınca gerçekleştirilen tüm sorgulama işlemlerine ilişkin bilgilerin görüntülenmesi,
- Sahibi ve kullanmakta yetkili olunan web servislerde meydana gelen planlı ve plansız kesintilere ilişkin bilgilerin görüntülenmesi,
- Sistemde kayıtlı kurumlara SMS ve E-mail şeklinde kesintiler ile ilgili bildirim yapılması, tarafınca gönderilen ve tarafına gelen bildirimlerin görüntülenmesi.

MWSY yazılımında veri tabanı yönetim sistemi olarak MS-SQL Server kullanılmıştır. Sistemin veri tabanında bulunan tablolar kısa açıklamalarıyla birlikte aşağıda verilmiştir:

- Sisteme ait kullanıcı bilgilerinin kaydedildiği Tbl_Ana_Kullanici,
- Sistemde yer alacak yetkilerin tanımlandığı Tbl_Ana_Rol,
- Sistemdeki kullanıcıların hangi rollere sahip olacağı bilgilerinin tutulduğu Tbl_Ana_Rol_Kullanici,
- Sistemde yer alacak menülerin yer aldığı Tbl_Ana_Menu,
- Sistemde kayıtlı rollerin hangi menüleri görüntüleyeceği bilgilerinin tutulduğu Tbl_Ana_Rol_Menu,
- Sistemde kayıtlı kamu kurumlarına ilişkin bilgilerin tutulduğu Kuruluşlar,
- Sistemde verisini diğer kurumlarla paylaşacak kurumların hazırladığı web servis bilgilerinin tutulduğu WebServisler,
- Hangi kurumların hangi web servislere erişimde yetkili olduğu bilgisinin tutulduğu WebServisYetkileri,
- Hangi kurumlarca hangi web servis sorgularının gerçekleştiği bilgisinin tutulduğu Sorgulamalar,
- Web servislerde meydana gelen planlı veya plansız kesintilerin bilgilerinin tutulduğu Kesintiler,

- Kurumlarda manuel veya sistem tarafından otomatik olarak gönderilen SMS veya E-mail bildirimlerinin tutulduğu Bildirimler,
- Sistem tarafından gönderilen otomatik bildirimlerin hangi vasıtalarla ve metinlerle yapılacağının ayarlanmasını sağlayan OtomatikBildirimAyarlari,
- Windows Servislerin bilgilerinin tutulduğu WindowsServisAyarlari,
- Yönetim Sisteminde kullanılan veri türlerinin bütününün tutulduğu Tbl_Ana_TabloTip.

Yönetim Modeli için hazırlanan bir diğer önemli bileşen de her bir web servisten otomatik olarak veri çekecek olan Windows servislerdir. Windows servislerin kesinti tespitine yönelik çalışma mantığına ilişkin iş akış diyagramı Şekil 5'te verilmiştir.



Şekil 5. Windows Servis Çalışma Mantığına İlişkin İş Akış Diyagramı

Şekil 5'te gösterildiği gibi Windows servisler programlandıkları saatte çalışırlar ve görevlendirildiği web servisten veri çekmeyi denerler. Serviste kesinti var ve kesinti kaydı daha önce başlatılmışsa sadece sorgu kaydı atılarak işlem sonlandırılırken, kesinti kaydı başlatılmamışsa sorgu kaydı atıldıktan sonra kesinti kaydı başlatılır ve ilgililere serviste kesinti meydana geldiğine dair bildirim gönderilir. Serviste kesinti yok ve aktif kesinti kaydı mevcut değilse yine sadece sorgu kaydı atılarak işlem sonlandırılırken, aktif kesinti kaydı mevcut ise sorgu kaydı atıldıktan sonra, kesinti kaydı sonlandırılır ve ilgililere servisteki kesintinin sona erdiğine dair bildirim gönderilir. Veri tabanına kaydedilen kesinti kayıtları sayesinde kesinti tespit edildikten sonra kesintinin ne kadar devam ettiği bilgisi elde edilebilir.

3. BULGULAR

Bu bölümde, Yönetim Modelinin uygulanması sonucu web servislerde meydana gelen plansız kesintilerin ne kadar sürede tespit edileceğine ilişkin bulgulara yer verilmiştir.

Plansız kesinti tespit süresinin hesaplanması için 20 Şubat 2021 saat 00:00 ile 21 Nisan 2021 saat 00:00 arasında geçen 60 günlük sürede 20 adet plansız kesinti meydana geldiği varsayılmıştır. 20 adet plansız kesinti zamanları, iki tarih arasındaki zaman değerlerinden rastgele seçim yapılarak belirlenmiştir. Simülasyon ortamında geliştirilen Windows servislerin çalışma zaman aralıklarına

bağlı olarak kesintinin meydana geldiği süreden ne kadar süre sonra ilgili Windows servis sorgusunun gerçekleşeceği hesaplanmış ve böylece söz konusu kesintinin ne kadar sürede tespit edildiği ortaya konmuştur.

Windows servisler her günün başında saat 00:00'da çalıştırılmış ve çalışma zaman aralıkları 24 saat, 12 saat, 6 saat, 3 saat, 1 saat, 30 dakika, 10 dakika, 5 dakika, 1 dakika, 30 saniye ve 15 saniye olarak ayrı ayrı değerlendirmeye tabi tutulmuştur. Çalışma zaman aralığı 24 saat olduğu durumda saat 00:00'da bir Windows servis sorgusu gerçekleştirildikten sonra bir sonraki sorgu bir sonraki gün saat 00:00'da gerçekleşecek, 12 saat olduğu durumda bir sonraki sorgu aynı gün saat 12:00'da gerçekleşecektir.

60 günlük zaman diliminde rastgele olarak belirlenen 20 kesinti zamanına göre, 11 farklı Windows servis çalışma zaman aralığında kesintilerin ne kadar sürede tespit edildiği ayrı ayrı hesaplanmıştır. Windows servis zaman aralığı 3 saatte 1 sorgu ve 15 saniyede 1 sorgu olduğu durumda hesaplanan kesinti tespit süreleri Tablo 1 ve Tablo 2'de örnek olarak verilmiştir.

Tablo 1. 3 Saatte 1 Windows Servis Sorgusu için Hesaplanan Kesinti Tespit Süreleri

Kesinti Numarası	Kesinti Tarihi (Gün, Ay, Yıl)	Kesinti Zamanı (Saat, Dakika, Saniye)	İlk İşlem Tarihi (Gün, Ay, Yıl)	İlk İşlem Zamanı (Saat, Dakika, Saniye)	Kesinti Tespit Süresi (Saat, Dakika, Saniye)	Kesinti Tespit Süresi (Saniye)
1	24.02.2021	23:46:40	25.02.2021	00:00:00	00:13:20	800
2	02.03.2021	19:59:45	02.03.2021	21:00:00	01:00:15	3615
3	04.03.2021	19:07:23	04.03.2021	21:00:00	01:52:37	6757
4	05.03.2021	10:58:42	05.03.2021	12:00:00	01:01:18	3678
5	05.03.2021	22:32:12	06.03.2021	00:00:00	01:27:48	5268
6	08.03.2021	09:37:11	08.03.2021	12:00:00	02:22:49	8569
7	09.03.2021	15:52:48	09.03.2021	18:00:00	02:07:12	7632
8	14.03.2021	03:57:46	14.03.2021	06:00:00	02:02:14	7334
9	19.03.2021	06:06:52	19.03.2021	09:00:00	02:53:08	10388
10	25.03.2021	07:19:59	25.03.2021	09:00:00	01:40:01	6001
11	25.03.2021	22:48:55	26.03.2021	00:00:00	01:11:05	4265
12	29.03.2021	16:18:07	29.03.2021	18:00:00	01:41:53	6113
13	01.04.2021	20:11:06	01.04.2021	21:00:00	00:48:54	2934
14	05.04.2021	05:53:41	05.04.2021	06:00:00	00:06:19	379
15	06.04.2021	22:27:44	07.04.2021	00:00:00	01:32:16	5536
16	09.04.2021	12:10:03	09.04.2021	15:00:00	02:49:57	10197
17	16.04.2021	14:24:27	16.04.2021	15:00:00	00:35:33	2133
18	18.04.2021	17:23:25	18.04.2021	18:00:00	00:36:35	2195
19	19.04.2021	07:20:11	19.04.2021	09:00:00	01:39:49	5989
20	20.04.2021	16:01:20	20.04.2021	18:00:00	01:58:40	7120

Tablo 2. 15 Saniyede 1 Windows Servis Sorgusu için Hesaplanan Kesinti Tespit Süreleri

Kesinti Numarası	Kesinti Tarihi (Gün, Ay, Yıl)	Kesinti Zamanı (Saat, Dakika, Saniye)	İlk İşlem Tarihi (Gün, Ay, Yıl)	İlk İşlem Zamanı (Saat, Dakika, Saniye)	Kesinti Tespit Süresi (Saat, Dakika, Saniye)	Kesinti Tespit Süresi (Saniye)
1	24.02.2021	23:46:40	24.02.2021	23:46:45	00:00:05	5
2	02.03.2021	19:59:45	02.03.2021	20:00:00	00:00:15	15
3	04.03.2021	19:07:23	04.03.2021	19:07:30	00:00:07	7

4	05.03.2021	10:58:42	05.03.2021	10:58:45	00:00:03	3
5	05.03.2021	22:32:12	05.03.2021	22:32:15	00:00:03	3
6	08.03.2021	09:37:11	08.03.2021	09:37:15	00:00:04	4
7	09.03.2021	15:52:48	09.03.2021	15:53:00	00:00:12	12
8	14.03.2021	03:57:46	14.03.2021	03:58:00	00:00:14	14
9	19.03.2021	06:06:52	19.03.2021	06:07:00	00:00:08	8
10	25.03.2021	07:19:59	25.03.2021	07:20:00	00:00:01	1
11	25.03.2021	22:48:55	25.03.2021	22:49:00	00:00:05	5
12	29.03.2021	16:18:07	29.03.2021	16:18:15	00:00:08	8
13	01.04.2021	20:11:06	01.04.2021	20:11:15	00:00:09	9
14	05.04.2021	05:53:41	05.04.2021	05:53:45	00:00:04	4
15	06.04.2021	22:27:44	06.04.2021	22:27:45	00:00:01	1
16	09.04.2021	12:10:03	09.04.2021	12:10:15	00:00:12	12
17	16.04.2021	14:24:27	16.04.2021	14:24:30	00:00:03	3
18	18.04.2021	17:23:25	18.04.2021	17:23:30	00:00:05	5
19	19.04.2021	07:20:11	19.04.2021	07:20:15	00:00:04	4
20	20.04.2021	16:01:20	20.04.2021	16:01:30	00:00:10	10

Tablo 1 ve Tablo 2'de yer alan Kesinti Tarihi ve Kesinti Zamanı kolonları, çalışma kapsamında belirlenen iki tarih arasından rastgele olarak seçilen kesinti zamanlarına ilişkin bilgileri göstermektedir.

Windows servis çalışma zaman aralığı 3 saatte 1 sorgu olacak şekilde ayarlandığında, Windows servis her gün 00:00, 03:00, 06:00, 09:00, 12:00, 15:00, 18:00 ve 21:00 saatlerinde sorgu gerçekleştirecektir. Tablo 1'e bakıldığında, 25.03.2021 saat 07:19:59'da kesinti meydana geldiği durumda Windows servis bu zamandan sonra ilk olarak saat 09:00:00'da sorgu gerçekleştireceği için kesintinin meydana geldiği saatten 1 saat 40 dakika 1 saniye sonra tespit edildiği görülmektedir.

Windows servis çalışma zaman aralığı 15 saniyede 1 sorgu olacak şekilde ayarlandığında, Windows servis her gün ilk olarak saat 00:00'da ve sonrasında her 15 saniyede 1 olacak şekilde sorgular gerçekleştirecektir. Tablo 2'ye bakıldığında, 25.03.2021 saat 07:19:59'da kesinti meydana geldiği durumda Windows servis bu zamandan sonra ilk olarak saat 07:20:00'da sorgu gerçekleştireceği için kesintinin meydana geldiği saatten 1 saniye sonra tespit edildiği görülmektedir.

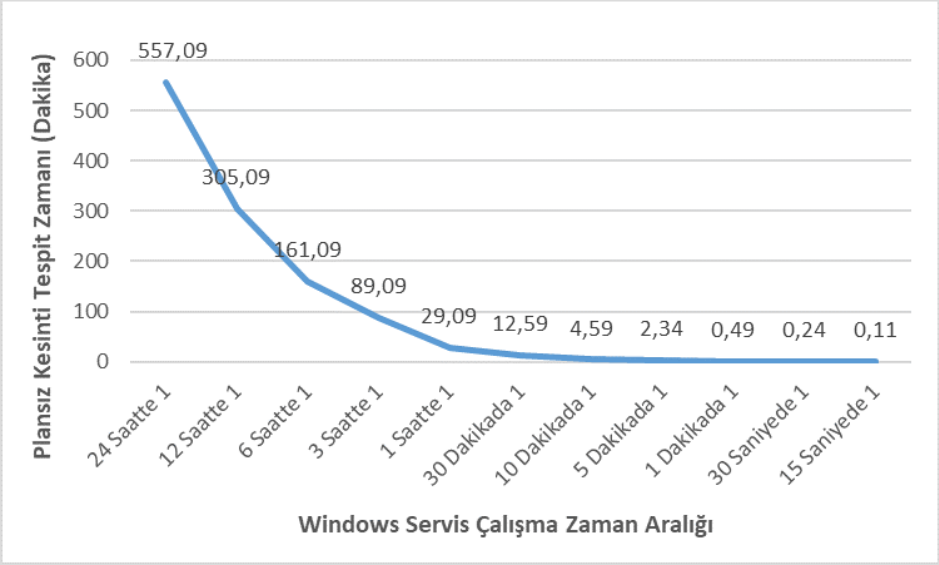
Çalışmada ele alınan 11 farklı Windows servis çalışma zaman aralığına göre 20 kesinti için elde edilen kesinti tespit sürelerine ilişkin olarak her bir çalışma zaman aralığında ortalama olarak kesintinin ne kadar sürede tespit edildiğine ilişkin veriler Tablo 3'te verilmiştir. Tabloda yer alan $\overline{x}$ sembolü, kullanılan yöntem ile kesintilerin ortalama kaç dakikada tespit edildiğini ifade etmektedir.

Tablo 3. Uygulanan Yöntemlerin Ortalama Kesinti Tespit Süreleri (Dakika Cinsinden)

Yöntem Numarası	**Windows Servis Çalışma Zaman Aralığı**	**Windows Servis Sorgusu ile Kesinti Tespiti ($\overline{x}$)**
1	**24 Saatte 1**	557,09
2	**12 Saatte 1**	305,09
3	**6 Saatte 1**	161,09
4	**3 Saatte 1**	89,09
5	**1 Saatte 1**	29,09

6	**30 Dakikada 1**	12,59
7	**10 Dakikada 1**	4,59
8	**5 Dakikada 1**	2,34
9	**1 Dakikada 1**	0,49
10	**30 Saniyede 1**	0,24
11	**15 Saniyede 1**	0,11

Tablo 3'e bakıldığında, Windows servis çalışma zaman aralığı 3 saat olarak belirlendiğinde 20 kesinti için ortalama olarak 89,09 dakikada kesintinin tespit edildiği görülmektedir. Benzer şekilde Windows servis çalışma zaman aralığı 15 saniye olarak belirlendiğinde 20 kesinti için ortalama olarak 0,11 dakikada kesintinin tespit edildiği görülmektedir. Plansız kesinti tespit süresinin Windows servis çalışma zaman aralığına göre değişim grafiği Grafik 1'de verilmiştir.



Grafik 1. Kesinti Tespit Süresinin Servis Çalışma Zamanına Göre Değişimi

Grafik 1 ve Tablo 3 değerlendirildiğinde Windows servis çalışma zaman aralığı kısaltıldıkça kesintinin ortalama olarak tespit edilme süresinin de kısaldığı görülmektedir.

4. SONUÇ

Bu çalışmada kamu kurumları arasında veri paylaşımında kullanılan web servislerde meydana gelen plansız kesintilerin kullanıcı sorgusu beklenmeden kısa sürede tespit edilmesi için Windows servislerden yararlanılmıştır. Veri paylaşımı için kullanılan her web servis için bir Windows servis geliştirilmiş ve söz konusu Windows servis belirli zaman aralıklarıyla web servislerden kesinti olup olmadığının tespiti için otomatik sorgu gerçekleştirmiştir.

Windows servisler için çalışma zaman aralığı web servislerde meydana gelen kesintilerin tespit süresinde önemli rol oynamaktadır. Çalışma kapsamında en uzun çalışma zaman aralığı 24 saatte 1 sorgu ve en kısa çalışma zaman aralığı 15 saniyede 1 sorgu olacak şekilde 11 farklı zaman aralığı üzerinde değerlendirme yapılmış ve çalışma zaman aralığı kısaldıkça kesinti tespit süresinin kısaldığı gözlemlenmiştir.

Kesintilerin en kısa sürede tespit edilebilmesi için çalışma kapsamında ele alınan zaman aralıklarından en kısa zaman aralığı olan 15 saniyede 1 sorgu ile Windows servislerin çalıştırılması

sağlanırsa, web servislerden gerçekleşecek sorgu miktarı ciddi oranda artacaktır. Windows servislerin çalıştırılma zaman aralığı ile Windows servisler tarafından gerçekleştirilen otomatik sorgu miktarının ters orantılı olduğu söylenebilir. Kurumların sahip oldukları uygulamaların kullanım sıklığına bağlı olarak diğer kurumlardan aldıkları web servisler için kesinti tolerans süresi belirlenmesi ve bu süreye uygun olacak şekilde Windows servis çalışma zaman aralığına karar verilmesi önerilmektedir. Belirlenen bu zaman aralıkları sayesinde kesintiler kullanıcı sorgusu gerçekleşmeden Windows servisler tarafından gerçekleştirilen otomatik sorgular ile tespit edilebilecektir.

KAYNAKÇA

Bacı, R. (2008). Development of a Web Services Security Architecture Based On .Net Framework. Yüksek Lisans Tezi. İzmir Yüksek Teknoloji Enstitüsü Mühendislik ve Fen Bilimleri Enstitüsü. İzmir.

Bakırov, A. (2012). Restful Web Service Security. Yüksek Lisans Tezi. Fatih Üniversitesi Fen Bilimleri Enstitüsü. İstanbul.

Balıkcı, F. (2014). Servis Odaklı Mimarilerde Web Servislerin Versiyonlanması için Bir Tasarım Yaklaşımı. Yüksek Lisans Tezi. Maltepe Üniversitesi Fen Bilimleri Enstitüsü. İstanbul.

Benharref, A., Serhani, M., Bouktif, S., & Bentahar, J. (2010). "A managerial community of Web Services for management of communities of Web Services". 2010 10th Annual International Conference on New Technologies of Distributed Systems (NOTERE). Tozeur: IEEE.

Deniz, E. (2009). Web Services Based Security Application Framework Model. İstanbul.

Devlet Planlama Teşkilatı (2009). Birlikte Çalışabilirlik Esasları Rehberi (2009). Ankara.

Gunawi, H., Hao, M., Suminto, R., Laksono, A., Satria, A., Adityatama, J., & Eliazar, K. (2016). "Why Does the Cloud Stop Computing? Lessons from Hundreds of Service Outages". SoCC '16: ACM Symposium on Cloud Computing, 1-16.

Gümüş, Ö., & Yürek, İ. (2015). "Anlamsal Web Servislerinin Dinamik Çağrımı". Bilişim Teknolojileri Dergisi, 71-87.

Kutlugün, E. (2018). Bilgi Sistemlerinde Hata Ağacı Analizi Yaklaşımı ile Risk Değerlendirme. Yüksek Lisans Tezi. İstanbul Arel Üniversitesi Fen Bilimleri Enstitüsü. İstanbul.

Oh, S.-C., Lee, D., & Kumara, S. (2008). "Effective Web Service Composition in Diverse and Large-Scale Service Networks". IEEE Transactions on Services Computing, 15-32.

Oliveira, R. A., Raga, M. M., Laranjeiro, N., & Vieira, M. (2020). "An Approach for Benchmarking the Security of Web Service Frameworks". Future Generation Computer Systems (110), 833-848.

Özdikililer, E., & Göksel, Ç. (2018). "Entegre Bilgi Sistemi Modeli Geliştirilmesi: DataOCEAN". Geomatik Dergisi (3), 225-232.

Rezaei Kalantari, K., Ebrahimnejad, A., & Motameni, H. (2020). "Dynamic software rejuvenation in web services: a whale optimization algorithm-based approach". Turkish Journal of Electrical Engineering & Computer Sciences (28), 890-903.

Sarıkoz, B. G. (2015). An Information Security Framework For Web Services In Enterprise Networks. Yüksek Lisans Tezi. Orta Doğu Teknik Üniversitesi Bilişim Enstitüsü. Ankara.

Sarıman, G., & Küçüksille, E. U. (2016). "Web Servislerinin Yazılım Güvenlik Testleri için Önerilen Hibrit Yaklaşım". SDU International Journal of Technological Science (8), 1-14.

Türk Standartları Enstitüsü. "Web Servis Güvenliği İçin Ortak Kriterler Koruma Profili, https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/2221/17032015140058-3.pdf, (20.09.2021).

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2017). "KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ", https://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm, (21.06.2017).

Yue, H., & Tao, X. (2012). "Web Services Security Problem in Service-oriented Architecture". 2012 International Conference on Applied Physics and Industrial Engineering, 1635-1641.