SETSCI Conference Indexing System,
Volume 3 (2018), 202-213

ISAS 2018-Winter
2nd International Symposium on Innovative Approaches in Scientific Studies
November 30 – December 2, 2018, Samsun, Turkey

Bulut Bilişimde Felaket Kurtarma Tekniklerinin İncelenmesi

Doç. Dr. Abdulkadir ÖZDEMİR[1], Baki GÖKGÖZ[2]

[1]Atatürk Üniversitesi, İktisadi İdari Bilimler Fakültesi, Sosyal Bilimler Enstitüsü, Erzurum, Türkiye
[2]Gümüşhane Üniversitesi, Bilgisayar Teknolojileri Bölümü, Torul Meslek Yüksekokulu, Gümüşhane, Türkiye

Özet-Günümüzde, bireysel ve kurumsal olarak çok büyük miktarda veri üretilmektedir. Üretilen bu verilere ihtiyaç olduğu anda ulaşılabilmesi ve üzerinde işlemler yapılabilmesi için bu verilerin çok iyi bir şekilde korunması gerekmektedir. Bu ise veri kaybına neden olabilecek olası felaket senaryolarında veri kurtarma hizmetlerini zorunlu kılmaktadır. Bulut Bilişim teknolojisi günümüz dünyasında yeni bir bilgi işlem platformu oluşturmuş durumdadır. Bulut Bilişim'in doğası gereği ana bulut üzerinde çok miktarda özel veri saklanmaktadır. Bu nedenle, veri kurtarma hizmetlerinin gerekliliği her geçen gün artmaktadır. Bununla birlikte verimli ve etkili bir veri kurtarma tekniğinin geliştirilmesine ihtiyaç duyulmaktadır. Kurtarma tekniğinin amacı, sunucu üzerindeki veriler kayba uğradığında veya kullanıcı sunucu üzerindeki verilere ulaşamadığı durumlarda, kullanıcının başka bir yedekleme sunucusundan ilgili verilere ulaşmasını sağlamaktır. Bu amaca ulaşmak için günümüze kadar birçok farklı veri kurtarma tekniği önerilmiştir. Bu çalışmanın amacı, bulut bilişim alanında kullanılan güçlü veri yedekleme ve kurtarma tekniklerini incelemektir.
Anahtar Kelimeler- Bulut Bilişim, felaket kurtarma teknikleri, veri güvenliği, yedekleme.

Examination of Disaster Recovery Techniques in Cloud Computing

Abstract- Nowadays, very large quantities of data are produced both individually and institutionally. These data must be preserved very well in order to be able to access and process them as needed. This situation necessitates data recovery services in possible disaster scenarios that could cause data loss. Cloud computing technology has created a new computing platform in today's world. A lot of private data is produced on the main cloud, which is the nature of Cloud Computing. These data can be vital information for individuals and institutions. For this reason, the necessity of data recovery services is increasing day by day. However, there is a need to develop an efficient and effective data recovery technique. The goal of the recovery technique is to ensure that the user has access to the relevant data from another backup server when the data on the server is corrupted and the user can not reach the data on the server. To this end, many different data recovery techniques have been proposed to date. The purpose of this study is to examine the powerful and useful data recovery techniques used in the field of cloud computing. The purpose of this study is to examine the powerful data backup and recovery techniques used in cloud computing.

Keywords- Cloud Computing, disaster recovery techniques, data security, backup.

1. GİRİŞ

Geçtiğimiz son bir kaç on yıl, bilgi işlemenin, internet üzerinden erişilebilen büyük bilgisayar ve depolama sistemlerinde, merkezi olarak daha verimli bir şekilde yapılabileceği fikrini pekiştirmiştir. Ağ oluşturma ve diğer alanlardaki ilerlemeler, iki yeni bilgi işlem modelinin kabulünden sorumludur. Bu durum, 1990'ların başlarında grid computing(dağıtık hesaplama) ve 2005'ten bu yana utility computing (yardımcı hesaplama) ve bulut bilişime yol açmıştır [1].

Utility computing de, donanım ve yazılım kaynakları büyük veri merkezlerinde yoğunlaşmaktadır. Kullanıcılar bilgi işlem, depolama ve iletişim kaynaklarını tüketirken ödeme yapabilmektedirler [1]. Utility computing kullanımı genellikle bulut benzeri bir altyapı gerektirir, ancak odak noktası, bilgi işlem hizmetlerini sağlayan iş modelidir. Bulut bilişim, Amazon, Apple, Google, HP, IBM, Microsoft, Oracle ve diğerleri gibi büyük BT şirketlerinin kullandığı utility computing benzeri bir yoldur [1].

Çok fazla çalışanı olan bir kuruluşta fiziksel donanımların kullanılarak cihazların veya lisanslı yazılımların kullanımı ve bu yazılımların herhangi bir gecikme olmaksızın tüm çalışanlara sunulması çok zor ve maliyetli bir iştir. Bu problemlerin üstesinden gelmek için bulut bilişim geliştirilmiştir. Bulut Bilişim; ağ, sunucu, depolama, uygulama ve servisler gibi düzenlenebilen bilgisayar kaynaklarına ait paylaşım havuzuna isteğe uygun olarak internet tabanlı erişimi sağlayan bir teknolojidir[2]. Bulut bilişim, internet alt yapısı kullanılarak erişim sağlanan yazılımsal ve donanımsal maliyeti düşüren, ölçeklenebilen, büyük miktarda veri depolanabilen, sanallaştırılabilen ortak bir alan teknolojisidir [3]. Daha genel bir tanım ile bulut bilişim, sistemlerin kaynak paylaşımı ile birbirine bağlı olduğu internet tabanlı bilgi işlem sürecidir. Herhangi bir istemci internete bağlanabildiği her yerden buluttaki verilere ulaşabilir veya verilerini bulut üzerinde depolayabilir.

2. FELAKET KURTARMA (DISASTER RECOVERY (DR)) NEDİR?

Herhangi bir kurum iş sürekliliğinin kesintiye uğramasını engellemek için kuruma ait verileri korumak ve bilişim sistemlerinin sürekli çalışmasını sağlamak zorundadır. Ayrıca altyapılarda meydana gelebilecek sorunlar kurumları telafisi olmayan felaketlere sürükleyebilir. Bu sorunların engellenmesi için kurum verilerinin tek bir merkezde tutulmaması dışında iş sürekliliğinin ana gereksinimlerinden bir tanesi de Felaket Kurtarma (Disaster Recovery) yönetimidir.

Bir sistemin herhangi bir sebepten çökmesi durumunda veri kaybı olasılığı vardır ve bazen bu durum finansal kayba neden olabilir. Bir sistemin insan hatası veya doğal afetler nedeniyle çökmesi durumunda kurum için maliyeti yüksek servis kesintilerine sebep olabilmektedir. Bu durum, iş sürekliliğinde bir felaket meydana getirebilir. Felaket olduğunda şirket olası veri kayıplarını göz önünde bulundurup verileri kayıplardan korumalıdır. Bulut hizmeti sağlayan Google, Amazon, Microsoft vb. şirketler bulut felaketi ve büyük miktarda veri barındıran sunucularda veri kaybı konusunda deneyimlidirler. Bir felaket durumunda eğer problem istemci tarafında ise veriler bulutta yedeklenecektir. Bu durumda istemci bazlı hizmet aksaması olabilmektedir fakat veri kaybı yaşanmamaktadır. Ancak bulutta meydana gelebilecek bir felaket durumunda veriler kaybolacaktır. Doğal afetler, ağ hatası, ağ saldırısı, kötü amaçlı yazılımlar, sistem hataları ve benzeri durumlarda felaketler meydana gelebilmektedir. Bu felaketlerin meydana gelmesi durumunda, veri kaybını önlemek için geliştirilen bazı felaket kurtarma teknikleri bulunmaktadır. Genel olarak bir ağda veya bulut servis sağlayıcılarda başarısızlığı önlemek için iki farklı felaket kurtarma modeli kullanılmaktadır. Bunlar; geleneksel ve bulut tabanlı servis modelleridir. Geleneksel model, özel altyapı veya dağıtılmış yaklaşım olarak kullanılabilmektedir. Hız ve maliyete bağlı olarak, müşteriler uygun modeli seçebilmektedirler. Özel yaklaşımda, bir müşteriye bir altyapı atanır, bu nedenle hem maliyet hem de veri kurtarma hızı yüksektir. Öte yandan, dağıtılmış modelde daha fazla kullanıcıya bir altyapı atanır. Bu yaklaşım, hem maliyeti hem de veri kurtarma hızını azaltır. Bulut tabanlı servis modelleri ise geleneksel felaket kurtarma ile karşılaştırıldığında düşük maliyetli bir hizmettir. Ayrıca fiziksel veya sanal olarak çoğaltmada esnek bir yapıya sahiptir. Bulut bilişimde sunucular arasında sürekli çoğaltma yapıldığından güvenlik, ağ bağlantısı ve sunucu yük devretme dahil olmak üzere sanal kurtarma ortamları için önceden oluşturulmuş seçenekler bulunmaktadır. Felaket kurtarma olarak buluttaki kritik sunucular ve veri merkezi alt yapısı çoğaltılmaktadır [4].

3. VERİ KAYBI NEDENLERİ

Felaket, sistem ömründe beklenmeyen bir olaydır. Doğal (tsunami ve deprem gibi), donanım/yazılım hataları (örneğin, 2011'de Amazon EC2'de barındırılan VM-VM'nin başarısızlığı) ve hatta insan (insan hatası veya sabotaj) ile yapılabilir. Bu durum ciddi mali kayıplara yol açabilir hatta insan hayatını riske atabilir [5]. Bu nedenle, büyük şirketlerdeki BT bütçesinin %2 ile %4'ü, her yıl Felaket Kurtarma için harcanmaktadır[6]. Bulut tabanlı Felaket Kurtarma çözümü, afetleri tolera etme, güvenilirlik ve kullanılabilirlik avantajları nedeniyle bu teknolojiye artarak devam eden bir yönelim vardır. Küçük ve orta ölçekli işletmelerde

(KOBİ'ler) daha yararlı olabilir, çünkü büyük şirketler gibi çok fazla veri kaynağına sahip değillerdir.

Her yıl birçok işletme çeşitli nedenlerden dolayı veri kaybı yaşamaktadır. Bu durumda herhangi bir felaket kurtarma yöntemi kullanmayan işletmelerin çoğunluğu bu verilerini kurtaramamaktadır. 2009 yılında blackblaze.com tarafından yapılan bir çalışmada, kullanıcıların %46'sının her yıl veri kaybına uğradığını ortaya çıkarmıştır [7]. Bu rakamı oluşturan en yaygın beş veri kaybı faktörü aşağıda maddeler halinde verilmiştir [8].

a) Doğal Afetler

Dünyada sel, deprem, kasırga, kar fırtınası, elektrik kesintisi ya da yapı tahribatından dolayı veri kaybına neden olabilecek doğal afetlerden etkilenmeyen çok az yer vardır. Ayrıca işletmenin konumuna bakılmaksızın, yangın her zaman göz önünde bulundurulması gereken bir risk türüdür. Bu nedenlerden dolayı bir Yedekleme ve Felaket Kurtarma çözümünde doğal afet riskleri düşünülerek bunlara karşı gerekli önlemler alınmalıdır.

b) Kritik Görev Uygulama Hatası

Bulut üzerinde bulunan ve kritik görevi olan bir uygulama birkaç günlüğüne kullanılamaz hale geldiğinde, bazı kuruluşlarda ani büyük bir hasara neden olabilir. Çözüm olarak bulutta depolanan uygulamalar kullanılarak ani büyük hasar azaltılabilir.

c) Ağ Hatası

Bulut Bilişim sisteminde istemciler internet ile buluta bağlanırlar. Bulut'a bağlanılan ağın çökmesi durumunda veriler kaybolacak ve bulut tabanlı çalışan uygulamalar da zarar görecektir.

d) Ağ Saldırısı

Kullanıcıların buluta bağlandığı ağdan worms(kurt), trojen, trafik taşma saldırısı, ara bellek taşma saldırısı vb. saldırılar gerçekleştirilebilir. Bu saldırılar sonucunda bir virüs uygulamalara bulaştığında, felaketin ortaya çıkmasına neden olabilir. Bu durumda bulutta virüsün bulaştığı yerde kullanılmayan uygulamalar bir izleme listesine yerleştirilerek, felaketin oluşması engellenebilir.

e) Kötü Amaçlı Kod

Bilgisayar korsanlarının veya kötü amaçlı kodun verileri değiştirmesi engellenmesine rağmen veri kaybı yaşanabilir.

f) Sistem Hatası

Bir buluta ait sistemin altyapısı başarısız olursa, o buluta bağlı tüm sistemler çökecektir. Sistem hatası felaketinin ortaya çıkmasının temel nedeni insandır.

4. GELENEKSEL FELAKET KURTARMA

Geleneksel felaket kurtarma, altı gruba ayrılan dağıtım grubu tarafından geliştirildi [3].

Seviye 0: felaket kurtarma planı ve kaydedilmiş veri olmadığı anlamına gelir. Kurum dışı veri yedeklemesi yoktur. Verileri kurtarmak için haftalar sürebilir ve başarısızdır.

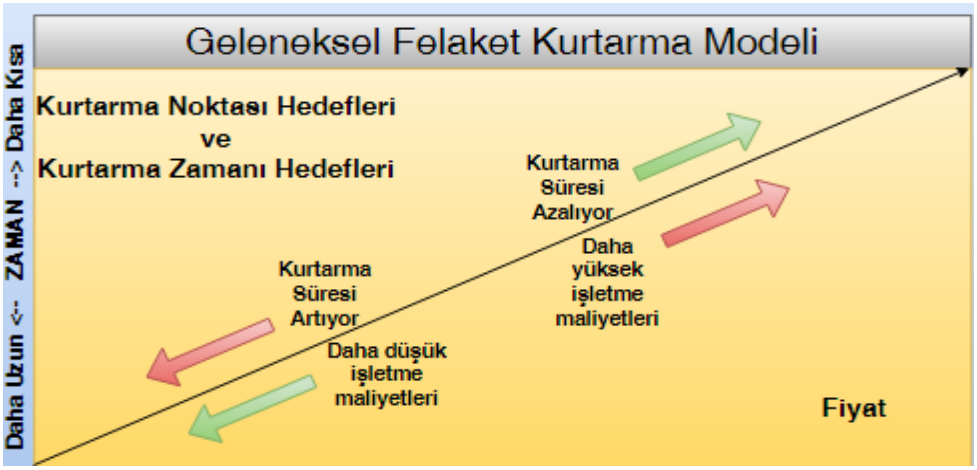
Seviye 1: hotsite (sürekli çalışan yedekleme alanı) olmayan veri yedeklemesi, verilerin hotsite tarafında değil, offsite (saha dışı yedekleme alanı) tarafında yedeklendiği anlamına gelir. Yedek alınan verilere ulaşmak zaman alır. Kendi yedek sunucularına sahip olmamaları nedeniyle, uygun sistemleri bulmak ve yapılandırmak için zaman kaybına neden olur.

Seviye 2: hotsite (sürekli çalışan yedekleme alanı) ile veri yedeklemesi, ana sistem çalışırken bu sistemin orijinal kopyası sürekli olarak başka bir yerde oluşturulmasıdır. Sürekli olarak çalışmakta olan bir yedekleme sitesi olarak tanımlanabilir. Sıcak Site çevrimiçidir ve hemen erişilebilir durumdadır.

Seviye 3: fiziksel araçlar tarafından yedek almak yerine, yedek bir veri ağının hotsite (sürekli çalışan yedekleme alanı) tarafından erişilebilir olması için bir elektronik kasa sağlar. Sıcak alan yedekleme maliyeti düşük olduğundan ağa erişmek daha iyidir.

Seviye 4: kısa zaman aralıklarında alınan kopyalar, kuruluşun daha fazla verisini koruduğu anlamına gelir. Bu kısa aralıklar ile alınan yedeklemelerde kuruluşa ait önemli veriler korunur.

Seviye 5: işlem bütünlüğü, işlemlerin üretim sistemleri ve kurtarma siteleri arasında tutarlı olduğu anlamına gelir. Yani, veri kaybı olmamalıdır.



Şekil-1 Geleneksel felaket kurtarma modeli şeması

5. GÜNÜMÜZDE FELAKET KURTARMANIN DURUMU

Günümüzde tipik bir Felaket Kurtarma servisi, uygulamalarını iki veri merkezi arasında eş güdümlü olarak çoğaltarak çalışır. Herhangi bir olumsuzluk durumunda sistemin çökmemesi için birincil veri merkezi kullanılamıyorsa, sistem yedekleme sitesini devreye alır ve en yakın zamanda kopyalanan verileri kullanarak uygulamanın en yeni kopyasını etkinleştirir. Bu durum, hizmet kesintilerini en aza indirirken, uygulamaların bir yedekleme sitesine geçmesine izin vermektedir.

5.1. FELAKET KURTARMA GEREKSİNİMLERİ

Bu bölümde etkili bir Felaket Kurtarma servisi için temel gereksinimler ele alınmaktadır. Bu gereksinimlerin bazıları, sistem kesintisi veya veri kaybının finansal maliyeti gibi ticari kararlara dayanabilirken, diğerleri doğrudan uygulama performansına ve doğruluğuna bağlıdır.

Kurtarma Noktası Hedefi(Recovery Point Objective(RPO)): Bir Felaket Kurtarma sisteminin RPO'su, herhangi bir arızadan önce en son yedeklemenin yapıldığı noktayı göstermektedir. Diğer bir ifadeyle muhtemel bir felaket zamanında riske edilen data miktarını temsil eden süre RPO olarak adlandırılır. RPO, arızanın meydana geldiği andan itibaren geriye doğru (yani geçmişe doğru) ifade edilir ve saniye, dakika, saat veya gün olarak belirtilebilir. RPO Felaket Kurtarma Planlamasında önemli bir noktadır

Kurtarma Süresi Hedefi (Recovery Time Objective (RTO): RTO, bir uygulamanın bir hata meydana geldikten sonra çevrimiçi olarak geri gelmesi için ne kadar süre geçmesi gerektiğini belirten dikey bir iş karardır. Bu, arızayı algılamak, yedekleme sitesinde (sanal veya fiziksel) gerekli sunucuları hazırlamak, başarısız uygulamayı başlatmak ve özgün siteden yedek siteye istekleri yeniden yönlendirmek için gereken süreyi içerir [9]. Diğer bir ifadeyle Kurtarma Süresi Hedefi (RTO), çalışmakta olan bir sistemdeki kesintiyle ilgili kabul edilemez sonuçlardan kaçınmak için, bir iş sürecinin bir felaketten sonra geri yüklenmesi gereken süre ve hizmet seviyesidir.

6. AFET KURTARMA ZORLUKLARI

6.1. Bağımlılık

Bulut hizmetlerinin dezavantajlarından biri, müşterilerin sistemi ve verilerini kontrol edememeleridir. Veri yedekleme, servis sağlayıcılarının kendi tesislerindeki sunucularda bulunmaktadır. Bu durum, müşteriler için (kurumlar gibi) bulut servis sağlayıcılarına (CSP) bağımlılık meydana getirmekte ve ayrıca felaket nedeniyle veri kaybı müşteriler için bir kaygı

nedeni olmaktadır. Bağımlılık [10], ayrıca güvenilir bir hizmet sağlayıcısı seçimi olan başka bir sorun meydana getirir.

6.2. Fiyat

Felaket Kurtarma (Disaster Recovery) hizmeti olarak bulut bilişimi seçmenin temel faktörlerinden birinin düşük fiyatı olduğu açıktır. Dolayısıyla, bulut servis sağlayıcıları her zaman farklı maliyet türlerini en aza indirerek kurtarma mekanizmalarını sağlamak için daha ucuz yollar aramaktadırlar. Felaket Kurtarma sistemlerinin yıllık maliyeti üç kategoriye ayrılabilir [11]:

- Başlangıç maliyeti: İtfa edilmiş yıllık maliyet
- Devam eden maliyet: Depolama maliyeti, veri aktarma maliyeti ve işlem maliyeti
- Potansiyel felaketin maliyeti: Düzelen afetlerin maliyeti ve ayrıca kurtarılamayacak felaketlerin maliyeti.

6.3. Hata Algılama

Başarısızlık tespiti süresi sistemin duruş sürelerini kuvvetle etkiler, bu nedenle hızlı ve doğru bir Felaket Kurtarma için mümkün olan en kısa zamanda bir hatayı tespit etmek ve rapor etmek çok önemlidir. Ayrıca, birden fazla yedek alma işlemi önemli bir sorundur. Ağ hatası ve hizmet kesintisinin ayırt edilebilmesi zordur.

6.4. Güvenlik

Daha önce de belirtildiği gibi, Felaket Kurtarma doğa tarafından meydana getirilebilir veya insan yapımı olabilir. Siber terör saldırısı, birçok sebepten dolayı gerçekleştirilebilen insan yapımı felaketlerden biridir. Bu durumda, önemli verilerin korunması ve geri kazanımı, sistem restorasyonunun yanında Felaket Kurtarma planlarında temel amaç olmalıdır.

6.5. Çoğaltma Gecikmesi

Felaket Kurtarma mekanizmaları yedekleme yapmak için çoğaltma tekniğine güvenir. Güncel çoğaltma teknikleri iki kategoriye ayrılır: senkron ve asenkrondur. Ancak, her ikisi de bazı avantajları ve dezavantajları vardır. Senkronize çoğaltma, çok iyi Kurtarma Noktası Hedefi (RPO) ve Kurtarma Süresi Hedefi (RTO)'ni garanti eder, ancak pahalıdır ve büyük yük yüzünden sistem performansını da etkileyebilir. Öte yandan, asenkron çoğaltma ile benimsenen bir yedekleme modeli daha ucuzdur ve aynı zamanda sistem düşük yüke sahiptir, ancak Felaket Kurtarma hizmetinin kalitesi düşecektir. Bu nedenle, maliyet, sistem performansı ve aynı

zamanda çoğaltma gecikmesi arasında işlem yapmak, bulut felaket çözümlerinde yadsınamaz bir sorundur.

6.6. Veri Depolama

İş veritabanı depolaması, bulut hizmetleri tarafından çözülebilen işletmelerin sorunlarından biridir. İşletmelerin artmasıyla birlikte işletmelerin bulut tabanlı depolarda büyük miktarda veri depolaması gerekmektedir. Geleneksel veri depolama cihazları yerine, bulut depolama hizmeti maliyetten tasarruf edebilir ve aynı zamanda daha esnektir. Bir bulut depolama sisteminin mimarisi dört katman içerir: fiziksel depolama, altyapı yönetimi, uygulama arayüzü ve erişim katmanıdır. Uygulamaları tatmin etmek ve verilerin güvenliğini garanti altına almak için donanım dağıtımı yapılmalı ancak depolama merkezileştirilmelidir. Bu nedenle, tek bir arıza noktasını ve veri kaybını depolamak, bulut servis sağlayıcılarında için kritik zorluklardır [12].

7. FELAKET KURTARMA ÇÖZÜMLERİ

7.1. Yerel Yedekleme

Bağımlılık sorunu için bir çözüm önerilmiştir [10]. Verilerin kontrolünü yapmak ve hem verilerin hem de uygulamaların eksiksiz yedeklenmesi için müşterilerin yanına bir Linux kutusu yerleştirilebilir. Yerel depolama güvenli bir kanal üzerinden güncellenebilir. Bu teknikle, bulut hizmeti sağlayıcıları arasındaki göç ve ayrıca kamuyla özel arasındaki ve özel sektörle kamu arasında göç mümkündür. Bir felaket durumunda, yerel yedekleme servis sağlayıcının sunduğu hizmetleri sağlayabilir.

7.2. Coğrafi Artıklık ve Yedekleme

Coğrafi artıklık geleneksel modelde kullanılabilir, ancak pahalı ve uygun değildir. İki bulut bölgesinin birbirinin bir kopyası vardır [12]. Bir bölgede problem yaşanırsa başka bir bölge açılır ve hizmetleri sağlar. Felaketleri tespit etmek için bölgeleri izleyen bir modül vardır. Birincil bölge, ekstra kaynak istemek veya kullanılmayan kaynakları serbest bırakmak için aktif bir yük dengeleyiciye sahiptir. İkinci bölge ayrıca pasif yük dengeleyicisine sahiptir. Başka bir araştırma [13] çoklu yedekleme için en uygun konumları seçmek için bir yöntem önerilmiştir. Uygulama sayısı ve hizmetlerin önceliğine göre yer sayısı belirlenir. Uzaklık ve bant genişliği, bu yöntemdeki en iyi alanları seçmek için iki faktördür. Bununla birlikte, bu çalışma, ayna

alanlarının kapasitesi ve her lokasyonda barındırılabilecek düğüm kaynağı sayısı gibi bazı kritik faktörleri göz ardı etmektedir.

7.3. Bireysel Bulut Depolama

Bu yaklaşım bulut veri depolama için önerilmiştir [13]. Depolama Ağı Endüstrisi Birliği verilerine göre, iş veri depolaması için en az üç yedek konum gereklidir. Kullanıcıların verileri üç farklı coğrafi konumda depolanmalıdır: Sunucular, Yerel yedekleme sunucusu ve uzaktan yedekleme sunucusudur

7.4. Kaynak yönetimi

Heterojen bulutlar, hibrid depolama ve çeşitli diskler gibi birçok farklı donanım ve yazılımı içerir. Bulut tabanlı işletmelerde, tüm iş verileri bulut depolama alanında depolanır. Dolayısıyla, bu ortamlarda veri koruma, güvenlik ve kurtarma kritik öneme sahiptir. Tehlikedeki veriler, birincil ana bilgisayarda işlenen ancak henüz yedek ana bilgisayarda bulunmayan verilerdir. Yani, felaket durumunda, depolama bulutlarında veri kurtarma için geliştirilmiş teknolojiyi kullanmak gerekir. Veri kurtarma için önerilen üç çözüm vardır [14]:

- Tehlikedeki verilerin kopyalanması için bir felaket durumunda en hızlı disk teknolojisini kullanmak.
- Bozuk sayfa eşiğinin değiştirilmesi: Diskin temizlenmesi için beklenmesi gereken RAM'deki bozuk sayfaların yüzdesi azaltılabilir [15].
- Riskli cihazların tahmini ve değiştirilmesi: Güç tüketimi, ısı dağılımı, karbon kredisi kullanımı ve verilerin önemi (her bir diskte saklanan) gibi belirli bazı faktörler belirli bir zaman diliminde hesaplanabilir. Bu faktörler ile öncelikli bir yedek listesi oluşturulmalıdır.

7.5. Pipelined Çoğaltma

Bu çoğaltma tekniği [16], hem asenkron replikasyonun performansını hem de senkronizasyonun tutarlılığını elde etmeyi amaçlamaktadır. Eşitleme çoğaltmasında, yedekleme, yedekleme yerinde tamamlanma tamamlanıncaya kadar devam edemez. Eşzamanlı çoğaltmada, yerel depodaki verileri sakladıktan sonra süreç başlatılabilir.

7.6. Yukarı / Aşağı Ölçeklendirme

Bazen, yüksek öncelikli işlevlerin yerine getirilmesi para kaybını azaltabilir veya bir felaket durumunda geliri artırabilir. Hizmetlerin önceliği, hizmet seviyesi anlaşması, gelir miktarı ve acil ihtiyaçlar gibi bazı farklı özellikler tarafından tanımlanabilir. Bir alanda doğal

bir felaket meydana geldikten sonra, bulut servis sağlayıcıları yoğun hizmet talepleriyle karşı karşıya kalmaktadırlar. Bu durumda servis sağlayıcılar mevcut kullanıcı hizmetlerini yönetmeli ve yeni kullanıcı isteklerini de üstlenmelidir. Servis sağlayıcılar mevcut kullanıcıları memnun etmeli ve mümkün olduğunca yeni müşterilere hizmet vermelidirler.

8. SONUÇ

Günümüzde bulut bilişim günlük yaşamda çok önemli hale geldi ve her şirket bulut bilişime dayanmakla birlikte buluttaki felaketlerden haberdar değillerdir. Herhangi bir sorunla karşılaştıklarında herhangi bir kurtarma mekanizmasını bilmiyorlar. Felaket meydana geldiğinde, tüm şirketler büyük bir veri kaybıyla karşı karşıya kalmaktadır ve birçok kurtarma mekanizmasının yürürlüğe girmesinden sonra da finansallaşmıştır. Bulut terminolojisi, PaaS, IaaS ve SaaS hizmetlerini, bulut kullanıcılarına altyapı, yazılım ve platform açısından kendi gereksinimlerine göre hizmet veren bir hizmettir. Böylece kullanıcı herhangi bir zorluk çekmeden bulut kullanabilir. Felaket Kurtarma yöntemini bulutta uygulayarak, bir sistem hatası veya doğal afetler yaşandığında veri kaybından kurtulmak mümkündür. Bu nedenle, iş sürekliliğinde Felaket Kurtarma'yı uygulayarak veri kaybını ortadan kaldırabilir.

REFERANSLAR

1. Dan C. Marinescu, Cloud Computing Theory and Practice
2. Mell P. & Grance T. (2011). thenistdefinition of cloudcomputing, NIST Special Publication 800-145
3. I. Foster, Y. Zhao, I. Raicu, S. Lu, "Cloudcomputingandgridcomputing 360-degree compared", Grid Computing Environments Workshop, Austin, 1-10, 2008
4. Mr. Akshay A. Gharat, Mr. Devendra E. Mhamunkar Disaster Recovery in Cloud Computing International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 5, May 2015
5. Kashiwazaki, H. (2012). Practicaluses of cloudcomputingservices in a Japaneseuniversity of theartsagainstaftermath of the 2011 Tohokuearthquake. Proceedings of the ACM SIGUCCS 40th annualconference on Special interestgroup on universityandcollegecomputingservices(pp. 49-52)
6. Prakash, S.,Mody, S., Wahab, A., Swaminathan S., &Ramani (2012). Disasterrecoveryservices in thecloudforSMEs. IEEE International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM) (pp. 139-144). http://dx.doi.org/10.1109/ICCCTAM.2012.6488087
7. M.J. Shoer, The 5 Most Common Causes of Data Loss, Internet & Telephone Blog. https://www.itllc.net/it/the-5-most-common-causes-of-data-loss/
8. Mr.A.Srinivas, Y.Seetha Ramayya, B.Venkatesh A Study on Cloud Computing Disaster Recovery International Journal of Innovative Research in Computer and Communication Engineering(Vol. 1, Issue 6, August 2013)
9. Kimberly Keeton, Dirk Beyer, Ernesto Brau, Arif Merchant, Cipriano Santos, and Alex Zhang. On the road to recovery: restoring data after disasters. European Conference on ComputerSystems, 40(4), 2006
10. Javaraiah, V. (2011). Back up for cloud and disaster recovery for consumers and SMBs. IEEE 5th International Conference on Advanced Networks andTelecommunicationSystems (ANTS) (pp. 1-3). http://dx.doi.org/10.1109/ANTS.2011.6163671
11. Alhazmi, O. H., & Malaiya, Y. K. (2013). Evaluating disaster recovery plans using the cloud. Reliability and Maintain ability Symposium (RAMS), IEEE ProceedingsAnnual(pp. 1-6). http://dx.doi.org/10.1109/RAMS.2013.6517700
12. Pokharel, M., Lee, S., & Park, J. S. (2010). Disaster Recovery for System Architecture using Cloud Computing. 10th IEEE/IPSJ International Symposium on Applications andthe Internet (SAINT) (pp. 304-307).
13. Khan, J. I.,&Tahboub, O. Y. (2011). Peer-to-Peer Enterprise Data Backupover a Ren Cloud. IEEE 8th International Conference on Information Technology: New Generations (ITNG) (pp. 959-964). http://dx.doi.org/10.1109/ITNG.2011.164
14. Patil, S. R.,Shiraguppi, R. M., Jain, B. P., & Eda, S. (2012). MethodologyforUsage of Emerging Disk toAmeliorateHybrid Storage Clouds. IEEE International Conference on

Cloud Computing in EmergingMarkets (CCEM) (pp.1-5). http://dx.doi.org/10.1109/CCEM.2012.6354615

15. Rudolph, C. G. (1990). Business Continuation Planning/Disaster Recovery: a Marketing Perspective. IEEE Communications Magazine, 28(6), 25-28.

16. Wood, T.,Cecchet, E., &Ramakrishnan, K. K. (2010). Disasterrecovery as a cloud service: Economicbenefits&deploymentchallenges. 2nd USENIX Workshop on Hot Topics in Cloud Computing (pp. 1-7).