BULUT BİLİŞİMİN KURUMSAL ZORLUKLARI VE ÇÖZÜM ÖNERİLERİ

Yasin İNAĞ, Eyüp Burak CEYHAN, Şeref SAĞIROĞLU
Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, ANKARA
yasininag@gmail.com, eyupburak@gmail.com, ss@gazi.edu.tr

***Özet*—Son yıllarda veri saklama, sistem yönetme ve veriye ulaşma bulut bilişim teknolojisi ile sağlanmaya başlanmıştır. Yeni nesil cihazlarda donanımsal maliyet ve gereksinimleri azaltmak için sanal sunucular kullanılmaktadır. Kurumsal şirketler maliyet, yönetim ve bakım kolaylığı gibi sebeplerden dolayı bulut bilişimi tercih etmektedir. Bulut bilişim kullanıcı odaklı güvenlik açıklarını ortadan kaldırmaktadır fakat farklı güvenlik sorunları da mevcuttur. Fiziksel sunucular üzerinde kurulan sanal sunucuların yönetimi ve güvenliği önemlidir. Çoklu erişim ile birden fazla kullanıcının aynı anda farklı yerlerden erişim sağladığı sunucuların güvenliği ve kullanıcılara sağlanmış olan sanal sunucuların yönetimi farklı sorunlar meydana gelmesine sebep olmaktadır. Bellek yönetimi, sanallaştırma, kullanıcı veri güvenliği, veri gizliliği ihlalleri gibi yönetimsel sorunlar farklı yöntemler ile çözümlenmektedir. Bulut bilişimde, sanallaştırma, ortak altyapı kullanma, bellek yönetimi ve farklı ülkelerin farklı yasalarından kaynaklı zorluklar bulunmaktadır. Karşılaşılan sorunlar, sebepleri ve çözüm önerileri çalışmamızda sunulmuştur.**

***Anahtar kelimeler*— Bulut bilişim, Bellek yönetim, Çözüm önerileri, Karşılaşılan zorluklar, veri güvenliği**

***Abstract*-- In recent years, cloud computing is used for data storage, system management and accessing data. Virtual servers are being used on new generation devices to reduce hardware cost and requirements. Corporate companies prefer cloud computing for its cost, management and easy maintenance reasons. Cloud computing eliminates user-oriented sense of vulnerability. However, it has different security issues. Managing and securing virtual servers on physical servers are crucial. Accessing to these servers at the same time by multiple users from different locations might cause some security issues and management problems. Administrative issues such as memory management, virtualization, user data security, data privacy violations are resolved by different methods. In cloud computing, there are some difficulties in virtualization, using shared infrastructure, data management and different laws in different countries. This study presents current problems, its reasons and possible solutions.**

***Index Terms*— Cloud computing, Storage management, solution recommendations, the difficulties encountered, data security.**

I. GİRİŞ

Veriye ulaşmanın ve iletişimin hızla arttığı günümüzde erişimin mekandan bağımsızlaşması için farklı teknolojiler geliştirilmiştir. Bulut bilişim bu teknolojilerden biridir. İnternet alt yapısının gelişmesi ve geniş bant iletişimin sağlanması, yaygınlaşması ve ucuzlaması ile kullanımı yaygınlaşmıştır. Yapısal olarak, sabit fiziksel sunuculara internet yardımıyla erişim sağlanmaktadır. Fiziksel sunucularda kurulan ve yönetilen sanal sunucular ile kullanılır. Çoklu erişim yöntemi ile aynı anda farklı yerlerden farklı kullanıcıların erişimi sağlanmaktadır. İnternet erişiminin olduğu her yerden erişim mümkündür.

Bulut bilişimin daha ucuz ve güvenilir bir sistem olması, bakım onarımının ve geliştirilmesinin kolay olması kurum ve kuruluşlar tarafından tercih edilmesinin sebeplerindendir. Yönetimin kolay, maliyetin ucuz olduğu bulut bilişimde kullanıcı taraflı güvenlik açıkları azaltılmaktadır. Fiziksel sunucular üzerinden kurulan sanal sunucular ile teknoloji bağlantısı 7/24 sağlanmaktadır.

Farklı kullanıcı özellikleri ve aynı güçte tek sunucu üzerinden sanallaştırma kullanılarak hizmet verilmesi, kullanılmayan donanımsal ve yazılımsal maliyetleri engeller.

Bulut bilişimin yönetimi kolay olmasına karşın, güvenlik yönetimi tecrübe ve dikkat gerektirmektedir. Yetki, sanallaştırma, bellek üniteleri yönetimi, saldırı tespit ve sistem geri yükleme gibi durumlarda farklı sorunlar ortaya çıkmaktadır. Mimari yapı ve yetkilendirme, yazılımsal ve süreklilik, dokümantasyon ve yasal eksiklikler karşılaşılan başlıca sorunlardır.

Çalışmada karşılaşılabilecek sorunlar ve çözüm önerileri açıklanmıştır. Çalışmanın ikinci bölümünde bulut bilişimin teknik ve yazılımsal alt yapısı açıklanmıştır. Üçüncü bölümde literatürde karşılaşılan sorunlar üzerinde durulmuştur. Dördüncü bölümde karşılaşılan sorunlara karşı alınacak önlemler belirtilmiştir. Sonuç bölümünde ise kurumların bulut bilişimden yararlanırken dikkat etmesi gereken hususlar sunulmuştur.

II. BULUT BİLİŞİM

Teknolojinin hızla gelişmesi ile birlikte iletişim ve veriye ulaşmak da kolaylaşmaktadır. Veri, program ve yönetimsel araçlar artık sabit sunucularda saklanmamaktadır. Bulut bilişim olarak adlandırılan yapı ile kurumsal ve kişisel veriler sanal sunucularda tutularak zaman ve mekân kısıtlaması sorun olmaktan çıkmıştır. Bulut bilişim için farklı tanımlamalar yapılmıştır. Bulut bilişim, hesaplama ve bilgi hizmetleri iş modelidir. Birçok farklı yerde ve sayıda fiziksel veya sanal sunucular ile bilgiye ulaşmayı sağlayan bir disiplindir. Bulut bilişim daha az enerji harcanarak, daha kolay yönetim ve servis destekleyen bir teknolojidir [1]. Berkeley'e göre bulut

bilişim, veri merkezleri aracılığı ile birçok farklı modülde internet uygulamaları, servisler, donanım ve yazılımsal destek sağlayan teknolojidir [2]. Foster ve arkadaşlarına göre bulut bilişim, internet alt yapısı ile ulaşılan geniş ölçekli, dinamik, ölçeklenebilen, büyük veri depolama alanına sahip, sanallaştırılabilen ve daha az maliyetli bir iletişim ve ortak alan teknolojisidir [3].

Bulut bilişim, sanal ortamda ulaşım sağlanan fiziksel sunucularda tutulan verilere ve uygulamalara bilgisayar, mobil cihazlar veya diğer teknolojiler ile ulaşılmasıdır. Geniş bant ağ teknolojisinin ve ülke genelinde internet alt yapısının gelişmesiyle birlikte kullanımı artmakta ve kolaylaşmaktadır. Birçok kurum ve kuruluş bulut teknolojisinden faydalanmaktadır. Lisans ve bakım işlemlerinde kolaylık sağladığı gibi maliyeti de azaltmaktadır [3].

Sanallaştırma makineleri ile bir sunucu üzerinden yayın yapılarak tek bir lisansla kullanıcıya hizmet sağlanabilmektedir. Eğitim kurumlarındaki bilgisayar laboratuvarlarında, sanal makine ile sunuculara bağlanılarak kasasız, daha geniş depolama alanına sahip, daha güçlü bilgisayarlar olarak kullanılmakta, lisans ve bakım maliyetlerinden de önemli ölçüde kazanç sağlanmaktadır.

İnternetin ve bilgi toplumunun gelişmesi ile bulut bilişim kaçınılmaz bir teknoloji olmuştur. Büyük şirketler, kuruluşlar ve kişiler tarafından kabul edilen ve dağıtık bilgi işleme teknolojisinin yerine kullanılan yeni teknolojidir [4].

Bulut bilişim uygulamaları ve alt yapısı sanallaştırma teknolojisi üzerine inşa edilmiş bir yapıdır. Sanallaştırma, donanımların daha etkin kullanılmasını, aynı anda birden fazla uygulamanın birden fazla kullanıcı tarafından kullanılmasına olanak tanır [5].

Bulut bilişim dinamik yapısı ile kullanıcı ihtiyaçlarına göre etkin kullanım sağlar. Kullanıcının ihtiyacına uygun verileri kullanmasını sağlayarak gereksiz işlemci yükü ve enerji kaybını önler [5].

Büyük veri setlerini ve güçlü sistemleri tek elden kontrol ederek ve erişim sağlayarak büyük bir ekonomik tasarruf sağlar. Her kullanıcı için ayrı depolama alanı, işletim sistemi, uygulamalar, lisanslamalar ve donanımların yerine, doğrudan yönetim sağlayan ve ihtiyaca göre dinamik alt yapı hizmeti sunan ve zamandan ve maliyetten tasarruf sağlayan sistemlerdir.

A. Bulut Bilişim ve Diğer Gelişmiş Teknolojiler

Bulut bilişim, bilim ve teknoloji ışığında bilişim alanlarına uygulanmaktadır. Paralel hesaplama, dağıtık bilgi işleme, kiralık sunucu hizmeti, yaygın hesaplama, yazılım servisleri ve sanallaştırma teknolojileri gibi gelişmiş teknolojilerin bulut bilişim ile ortak çalışma alanları vardır. Çalışmanın bu bölümünde gelişmiş teknolojiler ile bulut bilişim arasındaki benzerlikler ve farklılıklar açıklanmıştır.

Paralel Hesaplama, karmaşık ve çözümü zor olan bazı problemlerin, birçok küçük bilgisayarın bir araya gelerek eş zamanlı çalışması sonucu kısa zamanda çözülmesini sağlayan teknolojidir. Genellikle çözümü için yüksek performans gereken problemlerin çözümünde kullanılır.

Dağıtık bilgi işleme, sanallaştırmayı ve birden çok kullanıcının ortak bir yapıda çalışmasını sağlayan sistemdir. Dağıtık bilgi işleme, problemin çözümü için kullanılan veri setini farklı işletim sistemlerinin veya cihazların ortak kullanımını sağlayan sanal servis sağlayıcısıdır. Sanallaştırma daha güçlü ortak bir işlemci sistemi oluşturur. Dağıtık bilgi işleme teknolojisinde tek bir veri seti etrafında işlem yapan farklı kullanıcılar varken, bulut bilişimde büyük veri setinden faydalanan bağımsız kullanıcılar bulunmaktadır [4].

Kiralık sunucu hizmeti, kullanıcılara ait oluşmuş verileri incelemek için kurulmuş bir alt yapıdır. Kiralık sunucu hizmeti genellikle su, elektrik veya doğalgaz kullanımına göre oluşan faturaları oluşturmakta faydalanılan ortak kullanımlı kaynak sağlayıcısıdır. Kurumların hesap işlemleri, ortak sunuculara bağlanan kullanıcıların tüketim miktarı ve ödemesi gereken tutar gibi verileri sağlayan sanallaştırma teknolojisinin de kullanıldığı yapıdır. Bulut bilişim sadece kaynak sunmaktan ziyade veri iletimi, uygulama geliştirme ve yönetme gibi servisleri de içermektedir [5].

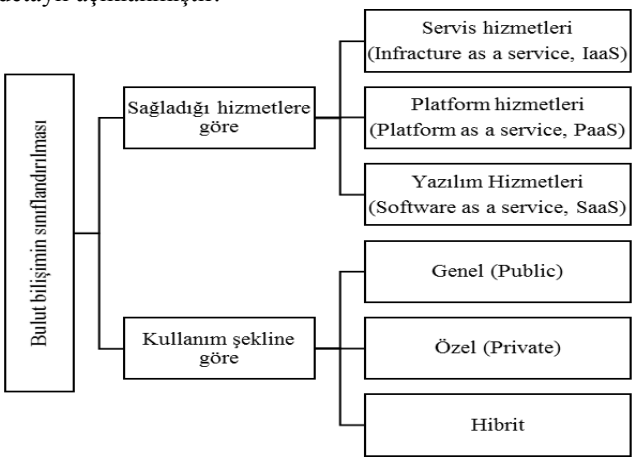
Dağıtık sistem birden fazla bilgisayarın aynı ağ üzerinde birbirleri ile etkileşimidir. Belirlenen amaç doğrultusunda ortak çalışan sistemlerdir [4].

Yazılım destekli servisler, paket yazılımların ortak kullanımına imkân sağlayan altyapı hizmetleridir. Sunucularda tutulan yazılımların kullanım ihtiyacına göre ortak kullanılmasına olanak tanıyan sistemdir. Uygulamalara erişimde sunuculara erişim ile olanak sağlandığından internet altyapısı olan her yerden ve her zaman ulaşılabilir [4].

Sanallaştırma, bilgisayar programlarının veya sistemsel yazılımların aynı donanım üzerinde çalıştırılabilmesidir. İşlemci sanallaştırma, tek işlemciyi çoklu işlemci gibi kullanmaya yarar ve aynı anda birden fazla uygulama veya işletim sisteminin kullanılmasını sağlar. Bu uygulamalar bellek ünitelerini birbirlerinden bağımsız kullanmaktadır. Bu yapılar bilgisayarın daha verimli kullanılmasını sağlar [5].

B. Bulut Bilişimin Sınıflandırılması

Şekil 1'de bulut bilişimin kullanım şekline ve verdiği hizmetlere göre sınıflandırılmıştır. Bu sınıflar alt başlıklarda detaylı açıklanmıştır.



Şekil 1. Bulut bilişimin sınıflandırılması [6].

Sağladığı hizmetlere göre sınıflandırma

Servis hizmetleri (Infracture as a service, IaaS), kullanıcıya sunulan donanımlardır. Fiziksel ve sanal sunucular, ağ, bant genişliği gibi servislerin son kullanıcıya ulaştırılmasını sağlayan yapıya IaaS denir. Kullanıcıların uygulamalarını ve düzenlerini sağlayabildiği yapıdır [6].

Platform hizmetleri (Platform as a service, PaaS), kullanıcıların uygulamalarını ve verilerini sakladığı alandır. Kişisel kullanım ayarlarının yapıldığı alandır [6].

Yazılım Hizmetleri (Software as a service, SaaS), kullanıcıların direk kullanabildiği yazılım ve program hizmet sağlayıcı birimidir. Veri saklamak için gerekli olan bellek ve yönetimi bu hizmet katmanı altında yer alır. Güvenlik ve sistem yönetimi gibi teknik alt yapılara destek sağlayan hizmet birimidir [6].

Kullanım şekline göre bulut bilişim

Bulut bilişim, güvenilirliği, kullanılabilirliği ve doğruluğu sağlamaktadır. Bunu her bir kullanıcı için ayrı ayrı yapılmasına gerek kalmaksızın gerçekleştirebilir [7]. Bu problemin çözümü için bulut bilişim genel (public), özel (private) ve hibrit(hybrit) olmak üzere üç ayrı kategoriye ayrılmıştır [8].

Genel (Public) bulut, kullanıcılar bulut sağlayıcıları tarafından her türlü bilgi ve belgeyi genelin kullanımına açarlar. Halka açık bir ağ topluluğu olarak da tanımlanabilir. Özel (Private) bulut, kurum veya kuruluşlara özel yapılandırılmış sistemlerdir. Üçüncü şahısların kullanımına kapalıdır. Hibrit (Hybrit) bulut, özel ve genel bulut mimarilerinin birlikte kullanıldığı bir yapıdır. Sistemin belirli kısımlarına sadece belirli kullanıcıların erişimine izin verildiği yapıdır.

C. Bulut Bilişimin Avantajları

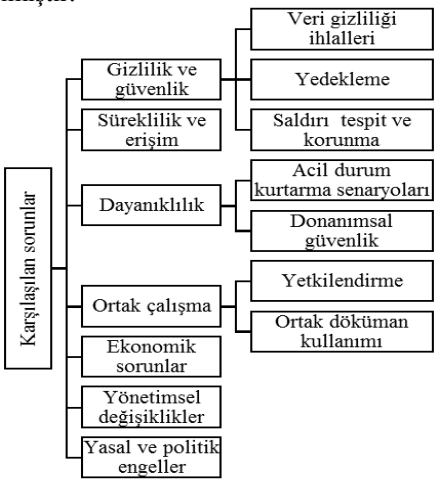
Kullanım alanına ve ihtiyaca göre dinamik yapı sergileyen bulut bilişim birçok kurum ve kuruluş için ekonomik tasarruf sağlamaktadır. Kişisel bilgisayarlar ile yapılan tüm işlemler bulutta da yapılabilmektedir. Bulut yapısı doğru yönetildiği sürece daha iyi performans elde edilebilir [9]. Her kullanıcı için ayrı ayrı alınması gereken programlar ve lisanslamalar tek bir yapı üzerinde oluşturularak ortak kullanıma açılır. Performans kaybı yaşamadan sanallaştırma yardımıyla aynı programdan birden fazla kullanıcı aynı anda yararlanabilir [8].

Yönetimde, sürdürülebilirlikte ve bakım çalışmalarında da büyük kolaylık sağlamaktadır. Herhangi bir yazılımın güncellenmesi gerektiğinde tek elden buluttan yapılan güncelleme ile kısa sürede ve kolayca yeni sürüm kullanıma sunulmuş olur. Yazılımsal ve donanımsal bakımın tek sunucu üzerinden yapılması büyük avantaj sağlamaktadır. Özellikle bilgisayar teknolojisinden anlamayan kullanıcılara sahip şirketlerde kullanılan uygulamalara gelen yenilikleri eklemede kullanıcı bazlı sorunlar yaşanmaktadır [10]. Bilgisayarların tek tek düzeltilmesi veya eğitimler ile yapılması gereken basit değişikliklerin bile anlatılması gerekmektedir. Bulut bilişim bu sorunu ortadan kaldırmaktadır Kurum veya kuruluşların farklı bölümleri için gerekli depolama alanı ihtiyaca göre farklılık göstermektedir. Bulut bilişimde dinamik bellek yapısından kaynaklı sorun yaşanmamaktadır [11].

Bir sunucuda bulunan verilerin farklı bir sunucuda da kopyası tutulmaktadır. Bu sebeple veri güvenliği sağlanmaktadır. Kullanıcı farkındalığı eksikliğinden kaynaklı oluşan hatalar ve sistem açıkları da bulut bilişimde engellenmektedir. Antivirüs ve benzeri uygulamalar etkin bir şekilde kullanılarak sistem ön güvenlik işlemleri gerçekleştirilir [12]. Bulut bilişimde kullanıcılar farklı işletim sistemleri kullanabilmektedir [7].

D. Bulut Bilişimdeki Zorluklar

Şekil 2'de bulut bilişimdeki karşılaşılan sorunlar sınıflandırılmıştır.



Şekil 2. Karşılaşılan sorunlar [10, 13-17]

Süreklilik ve erişim kullanıcılara sunulması gereken öncelikli hizmetlerdendir. Bulut mimarisinin 7/24 erişilebilir olması, sistemin süreklilik arz etmesi ve bu sürekliliğin sadece erişimde değil etkin performansta da olması gerekmektedir [14].

Sistemin olası bir saldırı veya afet durumunda dayanıklılığı, kurtarma senaryoları ve acil durum senaryolarının geçerliliği karşılaşılan zorluklardandır. Sel, deprem gibi doğal affet durumlarında alınmış önlemlerin güvenilirliği ve kurtarma stratejileri önem arz etmektedir [15].

Yetkilendirme, sisteme erişim hakkı olan kullanıcı veya profillerin sistemde müdahale sınırlarının ve öncelliğinin belirlenmesidir. Ortak çalışmada veri üzerinde değişiklik hakkına sahip farklı kademede birden fazla kişinin yetkisi bulunabilir [16]. Ortak doküman kullanımında aynı anda yapılan değişikliklerin gerçekleştirilmesi bulut bilişimin zorluklarındandır.

Ekonomik sorunlar kurumların bulut bilişimi tercih etmesinde önemli etmenlerden biridir. Bulut bilişim, kullanıcı odaklı kullanımdan dolayı daha düşük maliyetlidir. Ancak kendi yerel sistemini kullanan bir kurumun bulut bilişim mimarisine geçişi için gerekli maliyet gereksiz gelebilmektedir. Bu sebeple yapılacak olan analizlerde uzun vadeli planlar oluşturulmalıdır. Kısa vadede bir yük gibi görünse de uzun vadede kendini amorti edecek bir sistem olduğu gözlemlenmektedir [15].

Yönetimsel değişiklikler, kurumlarda değişen yöneticilerin farklı kararlar almasından veya gerekli dokümantasyon hizmeti sağlanmamasından projelerin değiştirilmesine sebep

olmaktadır. Yönetimin kapsama alanına giren her türlü yaklaşımda dokümantasyon işleyişin devamlılığı için önemlidir. Yönetimde bireylerin değişmesi farklı stratejileri beraberinde getirebilir. Önceki yapı bilinmeden yapılan değişiklikler veya ne yapıldığı bilinmeden uygulanan farklılıklar sorunlara sebep olabilir [17].

Veri gizliliği, kullanıcıların bulut ortamında sakladığı verileri üçüncü şahıslardan korumaktır. Kullanıcılara ait özel verilerin kötü niyetli kişilerden korunmasıdır. Sistemin geri bildirimini güçlendirmek veya sistemin reklam amaçlı kullanımı bile bazen kullanıcıların verilerinin gizliliği ihlal edilerek yapılmaktadır. Ülkelerin veri gizliliği ve korunması doğrultusunda aldığı kararlar farklılık gösterebilmektedir. Kullanılacak sunucuların bulunduğu ülke yasaları ile kullanıma açılan ülkelerin yasalarındaki farklılıklar sorun olarak gözlemlenmektedir [17].

III. BULUT BİLİŞİMDE GÜVENLİK SORUNLARI

Bulut bilişim, alt yapısı ve sağladığı olanaklar ile kullanıcılara daha ekonomik, kullanılabilir ve güvenilir sistemler sağlamaktadır. Bu yeni teknoloji birçok farklı mimariyi kullanıcı veya IT uzmanlarına sunmaktadır. Kullanılan sistem alt yapısı ve bulut teknolojisine göre farklı güvenlik riskleri oluşmaktadır. Hizmetin yanıt vermemesi, IP (Internet Protocol) çakışması, ortak donanım kullanılmasında yetki ve kullanım alanının sınırlandırılmaması, sanal ağlarda uygulamalara erişim, bellek ünitelerinin donanımsal bağımlılığının sanal ortamda ayrılmaması, saldırıların sunucuya bağlanan kullanıcılar tarafından gerçekleştirilebilmesi, web uygulamalarının ve web servislerinin yazılımsal açıklıkları karşılaşılan sorunlardır. Sanallaştırmada çoklu kullanıcı yapısı kullanıldığında farklı riskler ortaya çıkmaktadır. Birden fazla kullanıcının aynı veri havuzunu kullanıyor olması güvenlik risklerini artırırken sistemin kullanılabilirliği ve dinamik yapısını olumsuz etkileyebilmektedir. Web tabanlı kullanım sağlayan karakteristik yapıdan dolayı izinsiz erişim olasılığı normal web teknolojilerinden daha fazladır. Sanal sunucular arası geçişler ve paylaşılan platformun farklı yetkilere sahip kullanımlardan kaynaklı yönetimsel güvenlik açıkları da bulunmaktadır. Servis sağlayıcı hizmetleri platform tabanlı hizmetler ile bağımlı bir şekilde yazılım hizmetleri sunmaktadır [20, 21].

A. İletişimde Güvenlik Problemleri

Bulut servislerine internet altyapısı kullanılarak erişim sağlanmaktadır. Standart internet protokolleri kullanılarak iletişim gerçekleştirilir. İletişim, kullanıcılar ile bulut ve bulut bilişim sanal sunucuları arasında gerçekleşmektedir [22].

Kullanıcı ile bulut bilişim arasındaki iletişimden kaynaklı sorunlar; hizmetin yanıt vermemesi, ağ yönlendirme sorunları, ağın dinlenmesi, IP çakışması ve maskeleme gibi normal bir bağlantıda karşılaşılan sorunlardır. Ağ yönlendirme, kurulan altyapının yanlış konfigürasyonlar sonucu kısır döngüye girmesi veya yanlış sunuculara yönlendirilmesidir. Ağ dinlemesi, kullanılan alt yapıyı üçüncü şahısların gizlice izlemesi kişisel bilgi, görüşme ve ağ üzerinde gerçekleşen işlemleri elde etme çabasıdır. IP çakışması, kullanıcıların ağ üzerinde tanımlandırılan isimlerin aynı olması ve bu yapılandırmanın yanlış şekillendirmesinden kaynaklı oluşan sorunlardır [23-26, 28-29]. Bu problemlere çözüm önerileri; güvenlik soket katmanı, internet güvenlik protokolleri, şifreleme algoritmaları, denetleme, dijital sertifikalar ve trafik kontrolü gibi çözümlerdir.

Paylaşılan iletişim altyapısı

Ortak kaynak havuzu sadece veri ve uygulamaların kullanımı değil aynı zamanda ağ alt yapısının da ortak kullanımı demektir. Ağ bileşenlerinin ortak kullanılması çapraz kiracı (cross tenant) saldırılarına olanak sağlar. Çapraz kiracı saldırıları, ortak havuzda platform tabanlı servis sağlayıcıların kullanıcılara sağladığı, veri iletişim kanalları üzerinde gerçekleştirilen saldırı türüdür. Bulut bilişim kullanıcıları genellikle sanal sunucularına bağlanırken belirli bir kapasite ile sınırlıdır. Aşırı kullanım veya kötü niyetli kullanıcılar bu şekilde tespit edilmektedir. Sistem MAC ve IP adreslerini kayıt altına alarak sisteme sızmaya çalışan kötü niyetli ataklar engellenmektedir [26].

Sanal ağlar

Bulut bilişim sistemlerinde bağlantı sadece fiziksel ağ yapıları ile değil aynı zamanda sanal ağlar ile de gerçekleştirilmektedir. Sanal ağlar, sanal sunucular arasında iletişim gerçekleştirmek için tasarlanmıştır. Aynı hizmet sağlayıcısı üzerinde kurulu sanal sunucular arasındaki konfigürasyon, köprü kurma ve yönlendirme işlemlerini gerçekleştirmek için kullanılır. Sanal ağlar üzerindeki trafik fiziksel ağ üzerinden izlenememektedir. Bu sebeple sanal ağların güvenliği de fiziksel altyapı üzerinden gerçekleşmektedir. Saldırı tespit ve önleme mekanizmaları genellikle trafik izleme verisi üzerinden veya sistemsel anormallikler üzerinden anlaşılabilmektedir. Sanal ağlara saldırılar genellikle DoS, sızma veya dinleme ile yapılmaktadır. Bu saldırılarda sanal ağ kullanımı izlenerek tespit ve önlem gerçekleştirilir [23].

Hatalı güvenlik yapılandırılması

Bulut bilişimde kullanıcıya güvenli bir altyapı sağlamak oldukça önemlidir. Hatalı yapılandırma güvenlik ihlallerine sebep olabilir. Yaygın olarak yapılan hatalı yapılandırmalardan biri, yöneticinin almış olduğu güvenlik tedbirinin bütün sistemde geçerli veya bütün sistemle uyumlu olmamasıdır. Bulut sistemi güvenlik standartlarına uygun yapılandırılmalı ve denetlenmelidir. Dinamik yapıda yönetilmesi gereken, sistem yapılandırmadan kaynaklı dar boğaza girilmesi veri kaybına veya verinin ihlaline sebep olabilmektedir [28].

B. Mimari Güvenlik Problemleri

Bulut bilişimin donanımsal yapısından kaynaklı farklı sorunlar ortaya çıkmaktadır. Temelinde sanallaştırma teknolojisi kullanılan teknolide sanallaştırmanın yapılandırılması ve sanal sunucuların kullanıcı yetki sınırında kullanılması gerekmektedir. Bellek ünitelerinin güvenliği için, herhangi bir saldırı veya kayıp durumuna karşı geliştirilmiş kurtarma senaryoları geliştirilmelidir. Mimari yapının hataları

veya eksikliklerinden oluşan sorunlar çalışmanın devamında sanallaştırma, bellek üniteleri, kimlik yönetimi ve denetimi ve yasal sorunlar olmak üzere dört alt başlıkta açıklanmıştır.

Sanallaştırma

Sanallaştırma bulut bilişimin temel yapılarından biridir. Kullanıcılar kendi sanal makinelerini oluşturabilirler. Oluşturulan bu sanal makinede örneğin resim paylaşımı gerçekleştirilebilir. Ancak sisteme yüklenen resimlerin içerisinde kötücül yazılımlar yerleştirilmiş olabilir. Sanal sunucuda denetlenmesi zor olan bu yapı sebebiyle sanal makine zarar görebilir. Sanal makinenin gördüğü zarar, fiziksel donanım ve sanal ağlar ile tüm bulut sistemini de etkileyebilir.

Sanal makineler birbirinden bağımsızdır ve ayrı çalışabilmesi gerekmektedir. Aynı donanım üzerinde kurulu farklı sanal makinelerin bellek, işlemci ve diğer donanımların kullanımını ayırmaması durumunda sistem darboğaza girebilir. Bu da daha önce anlatıldığı gibi çapraz kiracı saldırısı olarak algılanıp sistemin çalışmasını engelleyebilir [21, 26].

Sanal sunucular sızıntı veya kaçış kötü niyetli kullanıcıların oluşturduğu ve bütün sanal makineleri kontrol eden mekanizmanın kontrolünden kurtulma amaçlı oluşturulan yapılardır. Makineler arası iletişim ve güvenlik protokollerini kontrol altında tutan mekanizma devre dışı bırakılarak veya bir makine gizlenerek sistemde güvenlik zafiyeti oluşturulabilir. Bu sızıntı ile fiziksel bellek ünitelerine erişim sağlanabilir [19].

Sanal makine göç sorunu güvenlik açıklarından biridir. Göç sorunu, sanal makine başka bir fiziksel makineye taşınırken sanal makinenin durdurulmamasından kaynaklı oluşabilecek ihlaldir. Sanal sunucu üzerindeki veriler, kodlar ve protokoller taşınma sırasında saldırıya uğrarsa her iki sanal makine de eksik kalacağından gerekli güvenlik prosedürü işletilemez olacaktır. Sanal makinelerde yapılan işlemleri geri alma daha önceden gerçekleşmiş güvenlik sorunlarını tekrarlayabilmektedir. Protokollerde yapılmış değişiklikler de etkilenebileceği gibi bu yapısal değişiklik bir ihlale sebep olabilir [22-25].

Bellek üniteleri

Bulut bilişim, sistemdeki verilerin erişim ve kontrolünü tam anlamıyla kullanıcılara bırakmaz. Sanal sunucuların etkin kullanımı ve yönetimi sağlanırken aynı durum veriler için geçerli değildir. Bulut içindeki verinin bütünlüğü, erişilebilirliği, gizliliği ve ihlalleri normal sistemlere göre daha az dayanıklıdır. Kullanıcı sayısı ve erişim miktarı arttıkça riskler de artmaktadır. Sadece sistemi bozmaya çalışan veri ihlali sağlayan yapılar değil, normal kullanımdan kaynaklı oluşabilecek darboğazlar da verinin bütünlüğüne zarar verebilir. Normal sistemlerden farklı olarak aynı bellek ünitesine birden fazla yoldan erişimin olması ve aynı anda farklı kişilerin bu belleklere erişebilmesi, normal fiziksel belleklerden daha riskli bir yapı oluşturmaktadır [28].

Veri kurtarma seçeneklerinden kaynaklı oluşan ihlaller bulut bilişimin veri güvenliği noktasında en önemli açıklarından biridir. Ortak bellek yapısını farklı kullanıcılar kullanmaktadır. Sanal sunucu üzerinden silinen verileri kurtarmak için uygulanacak yöntem ile işletim sistemi üzerinden görülmeyen ancak bellek adresleme tablolarında tutulan veriler kurtarılabilir. Ancak geri getirmek için gidilen adres başka şirket veya kişi tarafından kullanılan bellek bölgesi olabilir. Bir kullanıcıya veri kurtarma opsiyonu sağlayan sistem aslında bir başka kullanıcıya ait özel veriye erişim olanağı sağlamış olabilir.

Uzun zaman kullanılmayan veri setleri veya hasar görmüş bellek ünitelerini temizlerken, farklı kullanıcıların uygulamalarının buralarda açık olmasından kaynaklı silinemiyor ve temizlenemiyor olması, bir süre sonra farklı güvenlik ihlallerine yol açabilmektedir. Yedekleme işlemi veri bütünlüğünü korumak için önemlidir. Bulut bilişimde bellek üniteleri çoklu erişime ve kullanıma açık olmasına rağmen yedeklemenin direk erişime kapatılması olası bir saldırı veya zarar durumunda veri kurtarma olasılığını artırmaktadır [29].

Uygulamalar ve arayüz güvenliğinde karşılaşılan zorluklar

Bulut bilişime erişim web arayüzleri ile gerçekleşmektedir. Aynı web arayüzüne birden fazla kullanıcı eş zamanlı erişim sağlayabilmektedir. Hiyerarşik yapı ve yetki yönetiminin doğru yapılması güvenilirlik açısından önemlidir. Farklı kullanıcıların çoklu erişim desteği sayesinde bulut bilişimde kullandığı web uygulamaları sızıntılara ve saldırılara daha dayanıksız olmaktadır. Uygulamaların bulut bilişimde işleyişi ve çalışma prensibi kullanılan sistem hakkında bilgi verebilir [30].

Kimlik yönetimi ve erişim kontrolünde karşılaşılan zorluklar

Bulut bilişimde veri güvenilirliği ve bütünlüğü, kimlik doğrulama ve erişim kontrolü ile sağlanmaktadır. Sistemde yetkisiz erişimi engellemek ve girişimleri kayıt altında tutup analizler gerçekleştirmek oldukça önemlidir. Kullanıcı, yönetici ve sanal sunucularda, yöneticilerin farklı olmasından kaynaklı kontrollerin gerçekleşmesi zorlaşmaktadır. Aynı anda çoklu erişimin sağlanması, tek fiziksel yapı üzerine birden fazla sanal makinenin kurulması, dinamik bir karaktere sahip olması ve IP yapılandırması farklılığından kaynaklı kompleks bir yapı oluşmaktadır. Zayıf kimlik doğrulama ve erişim kontrolünden kaynaklı, hizmetlerin geç cevap vermesi, sanal makinelerin yeniden başlatılması, doğrulama kontrolünün yapılamaması, sistem günlüğü tutma ve izleme işlemlerinin yanlış veya gecikmeli yapılması gibi sorunların oluşmasına sebep olabilmektedir [23].

Sözleşme ve Yasalardan Kaynaklı Karşılaşılan Sorunlar

Bulut bilişim, altyapısı ve kullanım amacı doğrultusunda farklı coğrafyalardan kullanıcıların farklı ülkelerde bulunan sunuculara erişim sağlayarak gerçekleştirilen bir hizmettir. Bulut desteği sağlayan sunucuların, kullanıcılara önermiş olduğu sözleşmelerin kabul edilebilirliği, olası veri kaybı veya zararda nasıl bir yöntem uygulanacağı ve kimin nasıl sorumluluklar üstleneceği sözleşmede açıkça beyan edilmelidir. Sunucuların bulunduğu ülkelerin yasaları ile kullanıcıların kendi ülkelerindeki yasaların farklılığından kaynaklı oluşacak anlaşmazlıklarda hangi ülke yasalarının

geçerli olacağı bulut bilişim sorunlarındandır. Bu sebeple uluslararası geçerliliği olan ve bilirkişiler tarafından oluşturulmuş ortak bir yasanın geliştirilmesi ve kullanımı hızla gelişen ve yaygınlaşan hizmetin önündeki engellerden birini daha kaldıracaktır [17].

IV. GÜVENLİK SORUNLARINA ÇÖZÜM ÖNERİLERİ

A. İletişim Sorunlarına Karşı Önlemler

Bulut bilişimde uluslararası oluşturulmuş bulut güvenlik birliği ile sanal ve yerel ağlar, güvenlik duvarı ve IP yapılandırması gibi karakteristik altyapılar standartlaştırılmıştır. Bu standart, kullanıcı verilerini ve kullanılan sistem alt yapısının güvenliğini sağlamak için de kullanılır [31].

İleri bulut koruma sistemleri, bulut verilerini korumak için geliştirilmiş yüksek güvenlikli sistemlerdir. Kullanıcı odaklı ağ ataklarını engellemek için kullanılır. Servis sağlayıcıları tarafından sanal sunuculara yapılan saldırılar tespit edilerek önlenir. Bulut koruma sistemi iki farklı modülle çalışır. Birinci modülde saldırı izleme ve kayıt altına alma işlemleri gerçekleşirken ikinci modülde saldırı önleme işlemleri gerçekleştirilir. Sunucuların normal işleyişinde işlem süreleri ve kullanıcı sayıları kayıt altına alınır. Olası bir saldırı durumunda oluşan farklılık hemen kayıtlardaki MAC ve IP kayıt defterinden kontrol edilerek saldırı tespiti gerçekleştirilmiş olur. Saldırı tespiti yapıldıktan sonra ikinci modül devreye girer yapılan tüm saldırılar uyarı havuzunda kayıt altına alınır. Sistemin devamlılığı ile birlikte saldırının engellenmesini sağlamak için, kayıt defterinden tespit edilen anormal kullanıcıların sisteme erişimi engellenir [32].

İletişimde güvenlik için farklı yardımcı programlar kullanılmaktadır. Bunlardan biri CyberGuarder uygulamasıdır. CyberGuarder, sunucu üzerinde kurulu farklı sanal sunucular arasındaki iletişimin güvenliğini sağlamaktadır. Sanal sunucu yöneticileri üzerinden yapılan koruma işleminde sunucular arası iletişim uçtan uca (peer-to-peer) yaklaşımı ile gerçekleşmektedir. Bu yardımcı program ayrıca sanal sunucuların güvenliğinde de etkin rol almaktadır [33].

Bulut bilişim güvenliğinde kullanılan bir diğer yaklaşım *safeguard* güvenlik yapısıdır. Bu yapı ile fiziksel ve sanal sunuculara karşı gerçekleştirilen sızma ve izleme saldırılarına karşı önlemler alınmaktadır. Sanal sunucu yapılandırmasında direk olarak fiziksel sunucu ile birebir iletişim gerçekleştirilerek aracı yapılar engellenmektedir. Güvenlik senaryosunda yönlendirme, güvenlik duvarı ve paylaşım katmanı yapılandırmaları gerçekleştirilmektedir. Sanal sunucular üzerinden fiziksel sunucu ve ekipmanlarına gerçekleştirilen iletişim tek yönlü ve kontrollü gerçekleştirilerek güvenlik sağlanmaktadır. İletişim sağlanan her kanal belirli sabit tanımlayıcılar kullanılarak veri iletişim kontrolü paket iletişim ve doğrulama algoritmaları ile gerçekleştirilmektedir. Güvenlik duvarı ile paylaşım katmanına sızma engellenmektedir. Literatürde sanal sunucuların bağımsız çalışmasından kaynaklı oluşan sorunların çözümü için geliştirilmiş ve DCPortalsNg olarak adlandırılan sistem ile sanal sunuculara ait veriler haritalanmaktadır. Bu sayede ortak bellek ünitelerinden veri kullanımı eş zamanlı gerçekleşmesine rağmen veri paylaşımı ve erişimi sağlanmaktadır. Veri iletişimi paket olarak gerçekleştirilerek iletişimin doğruluğu kontrol edilebilmektedir. İletişimde herhangi bir ihlal durumunu tespit etmek için SnortFlow yaklaşımı kullanılmaktadır. Bu yapı kayıt defterlerini ve veri trafiğini izleyerek sakıncalı bağlantıların tespitini sağlamaktadır [31].

B. Mimari Güvenlik Sorunlarına Karşı Çözümler

Mimaride karşılaşılan sorunlara çözüm önerileri sorunlara göre sınıflandırılmış ve dört alt başlık altında toplanıp açıklanmıştır.

Sanallaştırmadan kaynaklı sorunlara karşı çözümler

Kurulan her sanal makineye güvenilir bir işletim sitemi kurulmalı, yardımcı güvenlik teknolojileri kurulmalı, sanal sunuculara bekleme veya başlatma şifresi oluşturulmalı, sanal sunuculara görüntü yüklendiğinde gerekli önlemler ve düzeltmeler yapılmalı ve bulut yapısı ile sanal sunucularda güvenlik araçları dahil edilmeli ve uygulanmalıdır [31].

Sanallaştırmada görüntü içerisine saklanan kötücül yazılımları engellemek için Mirage yaklaşımı kullanılmaktadır. Bu yaklaşım ile görüntü dosyaları hata ayıklama filtrelerinden geçirilerek kullanılır. Erişim kontrolü ile sağlanan yapıda görüntü dosyalarının bozuk kısımları veya içerisine saklanmış gizli programları temizleyerek veya engelleyerek sanal sunuculara yüklenmesine olanak tanınır. Görüntü içerisindeki kötücül yazılımlara karşı bir diğer yöntem görüntü dosyalarının AES şifreleme algoritması ile şifrelenmesidir. Oluşturulan şifre yönetim mekanizması ile şifrelenen metin sunuculara yüklendikten sonra yeniden şifre çözümleyerek elde edilir. Farklı bir yaklaşımda çevrimdışı olarak sanal sunuculardaki görüntüler kontrol edilmektedir. Yeniden yüklenerek filtrelemeden geçirilmektedir [34].

Fiziksel ve sanal sunucuların kullanım yetkileri farklı olmalıdır. Sistem erişimi için kullanılan yapı ve güvenilirliği ile sanal sunucuda kullanıcıların farklı yetki, şifre ve korunma yöntemlerine sahip olması güvenilirliği artırmaktadır. Bellek yönetimi ve sistem yönetimi servis sağlayıcı tarafından sağlanmalıdır. Kullanılabilirlik ve hız ile birlikte veriye erişimin saldırılara karşı korunmasının sanal sunucularda değil fiziksel sunucularda sağlanması gerekmektedir. Bunun için sanal sunucuların yönetimi fiziksel sunucu güvenlik ayarları ile kısıtlanmalıdır [35]. Sanal sunucular arası yönetimi sağlayan yapıda, sunucular arası veri iletişimi şifrelenerek gerçekleştirilir [36].

Cloudvisor, sanal sunucu yönetimi içerisinde iç içe sanallaştırma gerçekleştirerek hafif düzeyde güvenlik sağlayan nesne tabanlı sanallaştırma yöntemidir. Ayrışma (decoupling) modeli sanal sunucular çalışır durumdayken ortak kullanım ve donanımın yönetimini sağlayan yöntemdir. CPU, bellek üniteleri ve giriş-çıkış birimleri sanal sunucular arasında ortak kullanılan donanımlardır. Sanal sunucu yönetim birimi ile sanal sunucular arasındaki tüm iletişim ve paylaşım ve ayrışımı sağlayan ve güvenlik önlemlerini alan yapıya cloudvisor denir. Örneğin, sanal sunucu fiziksel sunucuda kaydını şifreli tutar ve gerektiği zamanlarda onaylamak için devreye koyar. Sanal

sunucuların kullanım alanını, erişim yetkilerini ve bellek tablolarının yönetimini sağlayarak çakışmaları önler. Şifreleme sanal sunucu üzerinde gerçekleştirilerek içerik koruma gerçekleştirilir. Merkel ağaç ve MD5 şifreleme algoritmalarını kullanır [37].

Kullanım aşamasında sanal sunuculara HyperCoffer güvenlik önlemi alınır. HyperCoffer sadece çekirdek tabanlı yapılan işlemleri güvenli görür ve geriye kalan donanımsal ve web arayüzlü kullanımlarda önlemler alır. Böylelikle HyperCoffer hem donanımsal hem yazılım olarak güvenliği sağlar. HyperCoffer sanal sunucuların birbirleri arasında ve fiziksel sunucular ile sanal sunucular arasındaki iletişimin kayıtlarını tutarak cloudvisor'dan daha geniş bir güvenlik sağlamaktadır [37].

Cloudsec yöntemi ile sanal sunucular üzerinden fiziksel bellekler ve donanımlar gözlemlenmektedir. İç gözlemeli bu yöntem ile saldırı tespiti sunucu çalışma zamanı içinde gerçekleştirilmektedir. Çekirdek tabanlı izlemede gerekli verilerin işleme alınması sağlanmaktadır. Aşırı değişim gösteren bellek ve işlemci değerlerine karşı önlem almada kullanılmaktadır [30].

Bir başka iç gözlemeli sanal sunucu mimarisi dışsal (exterior) olarak tanımlanmaktadır. Dışsal, özellikle misafir yani geçici sanal sunucular ile güvenli sanal sunucu arasındaki bağlantıyı sağlamada kullanılmaktadır. Misafir sanal kullanıcıların sürücü, bellek ve sistem dosyalarına erişimi engellenir [37].

Sanal sunucuların çalışma zamanında güvenliği sağlamak için bir başka yaklaşım, iletişim ve kopyalamada önlemler alan sanal güvenli platform modulüdür. (virtual trusted platform modula-vTPM). Hosting sağlayan sunucu ile sanal sunucu arasında kullanılan iletişim kanalının güvenilirliğini sağlamak için kullanılır. Aynı kanal birden fazla sanal sunucu tarafından aynı anda kullanılabilir. Şifreleme yapısı, süreklilik, güvenlik ve doğru iletişimi sağlamak için kullanılır [37].

Bellek ünitelerinden kaynaklı sorunlara karşı çözümler

Sanal sunucuların ortak kullandıkları bellek ünitelerinde, güvenliğin sağlanması için anahtarlama ile şifreleme yöntemleri kullanılmaktadır. Verilere erişimi ve sanal sunucuların bütünlüğünü bozmadan; güvenilir şifreleme algoritmaları, bellek yönetim yapısı ile kullanılabilirliği ve doğruluğu kabul görmüş güçlü şifreleme yöntemleri kullanılmalıdır [21].

Seccloud sadece sunuculara veri yüklerken değil sunucu içindeki veriler için de güvenlik sağlamaktadır. Arşivlenmiş verilerin güvenliği de şifrelenerek sağlanmaktadır. Yapısal olarak kullanıcı, bulut ve üçüncü kişiler için farklı anahtar yapısı kullanmaktadır. Sanal sunuculara veri yüklendiği zaman kişiye ait alana verinin kaydedilmesi önemlidir. Sisteme veri yükleyen kullanıcı kendine ait oluşturulan anahtarı ve bulut fiziksel sunucusu anahtarı ile sisteme veri yükleyebilir. Kişiye ait tasarlanmış alana kayıt gerçekleştirildiği zaman şifreli veri anahtarlar ile açılarak doğru adrese ve doğru kişinin erişimine açılır [38].

Sanal sunucularda tutulan veriler genel ise herhangi bir doğrulama ve güvenliğe ihtiyaç duyulmaz. Özel veri ise verinin saklandığı bellek indeksleri ve veri şifrelenerek saklanır. Sunucular bellek yönetimini genel ve özel olmak üzere iki farklı şekilde tanımlamaktadır. Üçüncü bir bölüm indekslerin tutulduğu yerdir ve erişim izni çok kısıtlıdır. Verilerin saklandığı alan da anahtarla şifrelendiği için olası veri kurtarma seçeneklerinde farklı kullanıcıların verilerine erişim engellenmektedir. Kişiye özel alan ve veri şifreleme gerçekleştiğinden, bellekten silinmiş verinin kurtarılmaya çalışılması sonradan o alana yüklenmiş veriye erişimi engeller [39].

Uygulamalardan kaynaklı sorunlara karşı çözümler

Bellek yönetiminde kullanılan anahtarlama yöntemi uygulamaya erişim ve kullanımda da geçerlidir. Uygulamaların güvenilirliği kullanıcıdan çok sistem yöneticileri tarafından sağlanan hizmetlerin güvenilirliği ile sağlanmaktadır. Saldırı modelleri sürekli yenilenmeli ve sistem güncel tutulmalıdır. Kullanılan yazılım ve uygulamaların güvenilirliği kontrol edilmelidir. Normal bilgisayar kullanıcılarının güvenlik duvarı ve antivirüs yazılımlarını kullandığı gibi uygulama hizmeti sağlayan servisler de kontrol edilmelidir. Sızma testleri sistem yöneticileri tarafından yapılarak sistemin güvenlik açıkları tespit edilip düzeltilmelidir [40].

Kimlik yönetimi ve erişim kontrolünden kaynaklı sorunlara karşı çözümler

Kimlik yönetimi ve erişim kontrolü bulut bilişimin yaygınlaşması ve kurumsal anlamda kullanılması için sağlanması gereken bir yapıdır. Şifreleme ve kişiye özel anahtar kullanılarak sisteme erişim ve kimlik denetimi farklı yöntemler ile gerçekleştirilmektedir [41]. Literatürde kişiye özel anahtar yerine kişiye özel ID veya şifrelenmiş kullanıcı adı gibi farklı tanımlar kullanılmıştır. Olası erişim sorunları, sunucu hataları ve uygulamaların çalışmaması gibi sorunlara karşı bulut bilişim, verileri farklı sunucularda yedekleyerek erişim sorununu çözmeyi amaçlamaktadır. Fiziksel sunuculardan kaynaklı oluşacak hataları ortadan kaldırmak için yedekleme ve acil durum yönetim hizmetleri sağlanmaktadır.

Sözleşme ve yasalardan kaynaklı sorunlara karşı çözümler

İnternet tabanlı oluşabilecek suçlara karşı dünya genelinde ortak kabul edilen bir yasa bulunmamaktadır. Bazı ülkelerin oluşturdukları ortak yasalar ve işbirliği geneli kapsamamaktadır. Bu sebeple hem internet ortamında işlenen suçlar hem de bulut bilişimde sunucuların yasa dışı saldırılarda hangi yasalara tabi olacağı bir muammadır. Ülkemizde yayın yapan internet sitelerinin yasa gereği sunucularını ülkemiz sınırları içerisinde tutması ve ülkemiz yasalarına uyması gerekmektedir. Bulut bilişimde veri yüklediğimiz ve kullandığımız uygulamalar için oluşturulmuş ortak bir yasa mevcut değildir. Bu sebeple bazı bulut hizmeti sağlayan kuruluşlar ülke yasalarına uygun altyapı ve fiziksel sunucu özellikleri belirlemektedir. Bulut bilişimde yaşanabilecek herhangi bir yasa dışı saldırı, normal internette işlenen suçlar kapsamında değerlendirilip Türk Ceza Kanunu hükümlerine göre cezalandırılır [42].

V. SONUÇ

Bulut bilişim hızla yaygınlaşan ve gelişen bir teknolojidir. Yakın zamanda bilgisayarlar bellek ünitelerinden bağımsız sanal sunucu bağlantısı sağlayan elektronik devreler ile yönetilecektir. Yerelde sanallaştırma ile kullanılan laboratuvarların yakın gelecekte tüm bilgisayarlar için geçerli olması kaçınılmazdır.

Gelişmekte ve yagınlaşmakta olan yeni teknolojinin karşılaşılan sorunlarının çözümü ve bulut yöneticilerine dikkat edilmesi gereken sorunlar karşısında farkındalık oluşturmak amacıyla sunulan çalışmada, karşılaşılan sorunlar alt başlıklar halinde sunularak karşılaşılabilecek sorunlara çözüm yolu bulmada kolaylık sağlanması amaçlanmıştır. Literatürde karşılaşılan sorunlara üretilen farklı çözüm önerileri derlenmiştir.

Bulut bilişimin kurumsal şirketler tarafından kullanılmasının ekonomik ve yönetimsel faydalarına ek olarak hizmet standartları, iletişim ve bilişsel faydaları sağlanmalıdır. Kurum çalışanlarını mekân ve zaman probleminden bağımsızlaştıran yeni teknolojinin stratejik faydalarının sağlanmasının güvenliği kurumlar için önemlidir.

Bulut bilişimin maddi ve yönetimsel olarak sağladığı kolaylık ve doğru yönetildiğinde üst düzey güvenlik sağlaması sebebiyle kurum ve kuruluşlarda da hızla yaygınlaşmaktadır. Google ve Windows gibi sektörün önde gelen şirketleri bulut teknolojisine büyük önem vermektedir. Windows Azure, Microsoft Office ve Google Drive gibi uygulamalar ve yatırımlar bunun en büyük kanıtıdır.

Bulut bilişimin temelinde sanallaştırma ve bellek yönetimi yatmaktadır. Sanallaştırmadan kaynaklı karşılaşılan güvenlik sorunları aslında ağ alt yapısında karşılaşılan sorunlar ile benzerlik taşımaktadır. Ancak bulut bilişim ve terimlerinin yeni olması farklı sorunlar gibi algılanmaktadır. Ortak ağda farklı işlemciler arkasında ve farklı güvenlik duvarları ve korunma yöntemlerine sahip bellek ünitelerinde ihlal durumu bulut bilişimden çok da farklı değildir. Sunulan çalışmada belirtildiği gibi bellek ünitelerinde ve veri kurtarma ve sanal sunucuya ait alan tablosu oluşturmada karşılaşılan zorluklar mevcuttur. Her sistemde olduğu gibi eğitimli ve donanımlı kişiler tarafından doğru kurulmuş ve yönetilen sistemlerde bu sorunlar çözümlenebilmektedir.

Bireysel kullanıcıların kiralama yöntemiyle kullandıkları sunucuların kontrolü farklı birim ve kişilerin elindedir. Oysa ki kurumsal bulut bilişim kendi sunucularını kullanabilmektedir. Maliyet politikası, iş zaman adam yönetimi ve teknolojiyi takip etmenin verdiği prestijlerin getirisi çok daha fazladır.

Bulut bilişimde ortak fiziksel sunucu kullanılması ve günümüzde tuş kaydedici (keylogger) gibi sunucu üzerinden kullanıcı bilgilerine ve kullanımlarına erişim sağlayan programların varlığı tehdit oluşturmaktadır. Kurumsal şirketlerin tamamının sunucu tabanlı ve yerel ağ tabanlı çalıştığı düşünüldüğünde, bulut mimarisinin daha güvenli olduğu gözlemlenmektedir. Bağlanmış olunan ağ kişinin bilgisayarının dünya ile bağlantısında mutlak uğrak noktası olduğu için her geçiş kaydedilip izlenebilmektedir. Oysa ki bulut bilişimde kullanıcı, sunucu üzerinde direk çıkış almakta ve güvenlik seviyesini kontrol etme yetkisi sunulmaktadır. Bu sebeple bellek yönetimi, veri güvenliği ve ihlal durumları açısından kurumsal bulut yapısının daha güvenli olduğu gözlemlenmektedir.

Kişilerin verilerini sakladığı ve büyük şirketlerin kontrolünde olan bulut teknolojisinin kötü amaçlı kişiler tarafından ele geçirilmesi ve veri gizliliği ihlallleri teknolojiye olan güveni azaltmıştır. Ancak kurumsal anlamda kullanılan bulut teknolojisinde sunucuların kontrolünün kurum görevlilerinde olması güven sorununu azaltmaktadır.

Sunucu kiralama yöntemi ile kullanılan bulut erişiminde sunucuların güvenliğinin kurumlarda olmaması, kiralama teknolojisine olan güveni azaltmaktadır. Bellek ve sunucu teknolojisinin gelişmesi ve ucuzlaması ile donanıma erişimin kolaylaşması, kurumların kendi alt yapısını kurmasına sebep olmakta ve karşılaşılan donanımsal sorunlara karşı kurum ihtiyaçlarına göre çözüm üretilebilmektedir.

Karşılaşılan sorunların teknolojinin doğru yönetilmesi ve kullanılması ile çözülebilecek sorunlar olduğu tespit edilmiştir. Kurumun ihtiyaçlarına göre tasarlanmış alt yapı ve bellek yönetimi ile maddi fayda sağlandığı gözlemlenmiştir. Bulut bilişimin sağladığı faydalara ek olarak doğru yönetildiği ve gerekli güvenlik önlemleri alındığında kullanıcı odaklı hataların azaldığı tespit edilmiştir.

KAYNAKÇA

[1] U. A. Kashif, Z. A. Memon, A. R. Balouch, J. A. Candio,"Distributed Trust Protocol for IaaS Cloud Computing", 12th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 275-279, 2015.

[2] M. Armbrust, A. Fox, R. Griffith, , A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "Above the Clouds: a Berkeley view of Cloud computing" Technical report, 2009.

[3] I. Foster, Y. Zhao, I. Raicu, S. Lu, "Cloud computing and grid computing 360-degree compared", Grid Computing Environments Workshop, Austin, 1-10, 2008

[4] Internet: HP Cloud research, http://www.hpl.hp.com/research/cloud.html Erişim Tarihi: 20.05.2015

[5] J. Gantz, D. Reinsel, "IDC's digital universe study (sponsored by EMC)", 2012.

[6] Internet: Amazon Elastic Compute Cloud, http://aws.amazon.com/ec2 Erişim Tarihi: 12.05.2015.

[7] Internet: Microsoft Azure, http://www.microsoft.com/windowsazure Erişim Tarihi: 10.05.2015.

[8] Internet: Eucalyptus Public Cloud, http://open.eucalyptus.com/wiki/Documentation Erişim Tarihi: 12.02. 2015.

[9] J. D. Lasica, "Identity in the Age of cloud computing: The Next-generation Internet's Impact on Business, Governance and Social Interaction" The Aspen Institute, 2009.

[10] S. Hackett, "Managed Services: An Industry Built on Trust", IDC, 2008.

[11] J. Staten, "Hollow Out The MOOSE: Reducing Cost With Strategic Rightsourcing", Forrester Research Inc., 2009.

[12] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, "Cloud computing - The business perspective" Decision Support Systems, 51 (1), 176-189, 2011.

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

[14] L.M. Vaquero, L. Rodero-Merino, J. Caceres, M. A. Lindner, "Break in the clouds: Towards a cloud definition", SIGCOMM Computer Communications Review, 39, 50-55, 2009

[15] M Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, "Above the Clouds: A Berkeley View of Cloud Computing" UC Berkeley Reliable Adaptive Distributed Systems Laboratory White Paper, 2009.

[16] G. Motta, N. Sfondrini, D. Sacco, "CLOUD COMPUTING: A business and economical perspective", International Joint Conference on Service Sciences, Shanghai, 18-22, 2012.
[17] W. Voorsluys, J. Broberg, R. Buyya, "Cloud Computing Principles and Paradigm", John Wiley and Sons, 2011.
[18] D. M. Parrilli, "Legal Issues in Grid and cloud computing, Grid and Grid Computing", Grid and Grid Computing, 97-118, 2010.
[19] M. G. Avram, "Advantages and challenges of adopting cloud computing from an enterprise perspective", Procedia tecnology, 12, 529-534, 2014.
[20] A. Corradi, M. Fanelli, L. Foschini, "VM consolidation: a real case based on openstack cloud", Future Generation Computer Systems, 32, 118–127, 2014.
[21] D.A.B. Fernandes, L.F.B. Soares, J.V. Gomes, M.M. Freire, P.R.M. Inácio, "Security issues in cloud environments: a survey", International Journal of Information Security, 13(2), 113–170, 2014.
[22] K. Hashizume, D.G. Rosado, E. Fernndez-Medina, E.B. Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, 4(5), 1–13, 2013.
[23] W.A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing", 44th Hawaii International Conference on System Sciences (HICSS), USA, 1–10, 2011.
[24] B. Liu, E. Blasch, Y. Chen, A.J. Aved, A. Hadiks, D. Shen, G. Chen, "Information fusion in a cloud computing era: a systems-level perspective", IEEE Aerospace and Electronic Systems Magazine, 29(10), 16–24, 2014.
[25] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, "Cloud computing the business perspective", Decision Support Systems, 51(1), 176–189, 2011.
[26] K.S. Rao, P.S. Thilagam, "Heuristics based server consolidation with residual resource defragmentation in cloud data centers", Future Generation Computer Systems,50, 87-98, 2015
[27] M. Song, "Analysis of risks for virtualization technology" Applied Mechanics and Materials, 539, 374–377, 2014.
[28] S. Subashini, V. Kavitha "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 1–11, 2011.
[29] J. Szefer, E. Keller, R.B. Lee, J. Rexford "Eliminating the hypervisor attack surface for a more secure cloud", in Proceedings of the 18th ACM Conference on Computer and Communications Security, 401–412, Chicago USA, 2011.
[30] Internet: Open Web Application Security Project Top 10-2013, The ten most critical Web application security risks, https://www.owasp.org/index.php/Top10 Erişim Tarihi: 08.05.2015.
[31] Internet: Cloud security alliance, security guidelines for critical areas of focus in cloud computing v3.0, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf Erişim Tarihi: 08.05.2015.
[32] F. Lombardi, R.D. Pietro, "Secure virtualization for cloud computing", Journal of Network and Computer Applications, 34(4), 1113–1122, 2011.
[33] J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, K.P. Lam, "Cyber-guarder: a virtualization security assurance architecture for green cloud computing", Future Generation Computer Systems, 28(2), 379–390, 2012.
[34] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, "Managing security of virtual machine images in a cloud environment", in Proceedings of the ACM Workshop on Cloud Computing Security, USA, 91–96, 2009.
[35] M. Kazim, R. Masood, M.A. Shibli "Securing the virtual machine images in cloud computing", in Proceedings of the ACM 6th International Conference on Security of Information and Networks, 425–428, Türkiye, 2013.
[36] D. Jeswani, A. Verma, P. Jayachandran, K. Bhattacharya, "ImageElves: rapid and reliable system updates in the cloud", IEEE 33rd International Conference on Distributed Computing Systems (ICDCS), 390–399, Philadelphia, 2013.
[37] F. Zhang, J. Chen, H. Chen, B. Zang, "Cloudvisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization", in Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, 203-216, 2011.
[38] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, "Security and privacy for storage and computation in cloud computing,", Information Sciences, 258, 371-386, 2014.
[39] Y. Tang, P.P. Lee, J.C.S. Lui, R. Perlman, "Secure overlay cloud storage with access control and assured deletion" IEEE Trans.on Dependable Secure Computing, 9(6), 903–916, 2012.
[40] S.K. Sah, S. Shakya, H. Dhungana, "A security management for cloud based applications and services with diameter-AAA", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, 6–11, 2014.
[41] S. Ruj, M. Stojmenovic, A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds", IEEE Transactions on Parallel & Distributed Systems, 25(2), 384–394, 2014.
[42] M.L. Hale, R. Gamble, "Secagreement: advancing security risk calculations in cloud services" IEEE Eighth World Congress on Services, Honolulu, 133–140, 2012.