Askerî Alandaki Bulut Sistemi Kullanımına Güvenlik Yaklaşımları

İsmail Aydın, Recep Kılıç, A. Zeki Gerehan

***Özet*—Bulut sistemi, günümüzün en gelişmiş sistemlerinden biridir. Hayatın her alanına giren bu teknoloji askerî alanda da kullanılmaktadır. Tüm ordular muharebe sahasını yönetmek için güvenlik ve teknoloji kullanımı dengesini koruyarak taktik resmi oluşturulmaya çalışmaktadır. Muharebe sahasındaki karmaşıklığın giderek artması önümüzdeki yıllarda taktik resmin oluşturulmasında daha fazla teknoloji ve daha fazla güvenlik tedbirleri gerektirecektir. Askerî alanda bulut sistemi kullanımı, sistemin karşılaştığı riskler ve bunlara karşı çözüm önerilerini içeren bir yazı takdim edilmiştir.**

***Anahtar Sözcükler* —Askerî uygulamalar, Bulut sistemi**

***Absract*— Cloud Computing is one of the most improvement system in the present-day. *This* technologies have become into all areas of life so that it's not without military. All armies in the world is try to make tactic picture, it's made for managing combat area, with using technology and security balance. While complexity in the field of battle is increasing, the next few years making tactic picture will be necessary more technology and more security protection. In this paper is presented using cloud computing in the military area, risks faced by the system and solving suggestions.**

***Index Terms* —Military applications, cloud computing**

I. GİRİŞ

BULUT sistemi her ne kadar net olarak tanımlanamasa da hayatın her alanında kullanılmaktadır. İnternetin askeri gereklilikleri karşılamak için oluşturulduğu düşünüldüğünde interneti aktif olarak kullanan bulut sistemi askeri uygulamalardan ayrı olması düşünülemez. Bulut sistemi, askerî uygulamalardan özellikle taktik resmin oluşturulması, ani durumların açıklığa kavuşturulması ve günlük rutin faaliyetlerin yürütülmesinde kullanılmaktadır. 1'inci Dünya Savaşı ile başlayan telsiz kullanımı, 2'nci Dünya Savaşı sonrası ihtiyaçları giderme maksadıyla ArpaNet'i ve daha sonra global olarak kullanılan İnternet ortaya çıkmıştır [1]. Ancak internetin askerî olmayan unsurlarca fazlaca kullanılması güvenlik açısından askeri kanadın başka yöntemlere başvurması gerekliliğini ortaya çıkarmıştır. Bu kapsamda maliyetlerin artması ve güvenlik hususları askerî kanadın bulut sistemini kullanmaya zorlamıştır. Askeri harekât açıdan çok önemli verilerin hem kullanabilir hem de güvenli olması dengesi bulut sistemini kaçınılmaz yapıp, yeni güvenlik risklerine karşı, yeni önlemler alma gerekliliğini yanında getirmiştir.

Askerî bulut sistemlerinin maruz kalabileceği riskleri 3 ana başlık altında toplamamız mümkündür. Bunlar;

A. Donanımsal Riskler

Alt yapı donanımlarının tahrip edilmesiyle, bütün verilerin kaybolmasına sebebiyet verecek risk kategorisi.

B. Yazılımsal ve İşletim Sistemleri Riskler

Bulut sistemini oluşturan yazılım ve işletim sistemlerinin güvenilir, minimum açıkları olan ve sürekli geliştirilebilen yazılımlar olmaması durumunda oluşabilecek risk kategorisi.

C. Kullanıcı Tarafından Meydana Gelen Riskler

Bilinçsiz kullanıcılar tarafından bulut sistemini zayıflatılacak ya da veri kaybına neden olabilecek siber saldırı girişleri yapılmasına müsaade edebilecek risk kategorisi.

II. BULUT SİSTEMİNİN TANIMI VE KAPSAMI

Bulut sistemi net bir tanımı bulunmamakla birlikte; uzak bir sunucu tarafından uygulamaların çalıştırılması ya da kullanıcı verilerinin sunucu tarafından her zaman ulaşılabilir şekilde bulundurulmasını sağlayan bir servis sistemi olarak tanımlayabiliriz. Bulut sistemi; basit ve kullanışlı ara yüzleri ile bilgiyi istenilen her yerde, istenilen zamanda ulaşılabilir ve kullanılabilir hale getirmiştir. 2000'li yılların başından itibaren, bilgilerin yerel bilgisayar diskinde bulundurularak yapılan uzak erişimler ve uygulamaların kullanıcı bilgisayarı üzerinden çalıştırılması ile merkezi bilgisayar ve ona bağlı terminal yapısı kullanılmaya başlanmıştır [2]. Bu yönüyle bulut sistemi; geçmişte kullanılmış bir yöntemin günümüzün ekonomik şartlarına uyarlanarak ve geliştirilerek, tüm ağ kullanıcılarının erişimine olanak sağlayacak şekilde yeniden sunulmasıdır [3].

Bulut sistemi ile bilgiye istenilen her yerden ve her türlü bilgi iletişim cihazı (PC, Mac, iPhone, Android veya BlackBerry) kullanarak ulaşmak mümkün olabilmektedir. Konuya askerî açıdan incelendiğinde daha çok ülkelerin kendi geliştirdikleri cihaz ve sistemlerle bilgiye ulaştıkları ve depoladıkları görülmektedir.

Yüksek erişilebilirlik imkânının sunulması, bellek ve disk değişikliği gerektirmeyen esnek yapının kullanılması ve doğa dostu (elektrik ve yer tasarrufu) olması, bulut sisteminin ilk bakışta dikkati çeken avantajları arasında görülmektedir.

İsmail AYDIN, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100/0100, İstanbul-Turkey, e-mail: iaydin2004@gmail.com.

Recep KILIÇ, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100/0100, İstanbul-Turkey, e-mail: rkilic40@gmail.com.

Ahmet Zeki GEREHAN, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100/0100, İstanbul-Turkey, e-mail: azgerehan@hotmail.com.

Bu avantajlı yönleri dikkate alındığında; bilgi iletişim teknolojilerindeki gelişimin yansıması olan bulut sistemiden uzak durmak ya da alternatif yöntemlerde ısrarcı olmak akılcı bir çözüm olarak görülmemektedir. Bulut sistemi beraberinde getirdiği avantajlar ile birlikte riskleri de unutulmamalı ve hassasiyetle üzerinde durulmalıdır.

A. Bulut Sistemi Modelleri ve Kullanım Biçimleri

Kullanım biçimine göre bulut sistemi üç sınıfta toplanmaktadır [4]. Bunlar (Şekil 1);

1. Genel Bulut (Public Cloud)

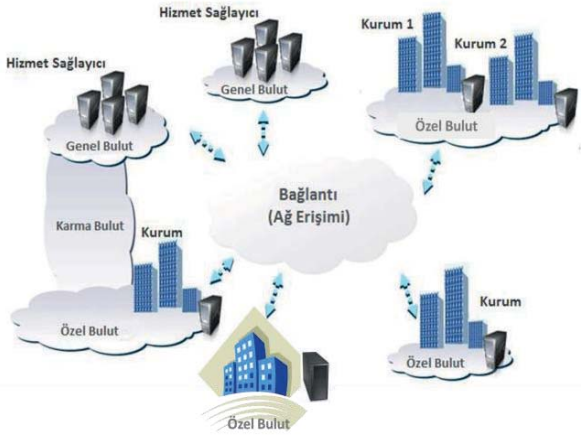
Web ara yüzü aracılığıyla internet üzerinden genel kullanıma sunulan hizmetlerdir (Google Apps, Amazon, Windows Azure) [5].

2. Özel Bulut (Private Cloud)

Belirli bir kurum ya da kuruluşa sunulan bulut hizmetidir. Bulut sistemini sağlayan, kurumun kendisi olabileceği gibi, başka bir bulut sistemi sağlayıcı da olabilir. Bu bulut sisteminde sadece kurum içi hizmet verilir.

3. Melez Bulut (Hybrid Cloud)

Genel ve özel bulut sistemlerinin birlikte kullanımasıdır. Bir kurumun verileri özel bulut içinde yer alırken, bazı servisleri genel bulut üzerinden halkın kullanımına açılabilir. Günümüzdeki askeri bulut sistemleri melez buluta örnek verilebilir.



Şekil 1. Bulut Sistemi Yapısı [6]

Bulut sistemi hizmet sağlayıcıları, bulut hizmetini sağlarken yazılım, platform ve alt yapı hizmet modellerinden birini ya da aynı anda birkaçını kullanmak zorundadır. Bulut Hizmet Modelleri aşağıda açıklanacaktır.

B. Bulut Sistem Hizmet Modelleri

1. Yazılım Hizmetleri (SaaS - Software as a Service)

Uygulama bulutudur. Bulut sistemi alt yapısı kullanılarak, web tabanlı çeşitli uygulama ve yazılımların (örneğin e-Posta, ağda konferans) bulut sistemi kullanıcısına sağlanmasıdır. Kullanıcı, bulut hizmeti almakta olduğu sunucu bilgisayar üzerindeki yazılımı çalıştırmak suretiyle istediği dosyaları üzerinde çalışabilmektedir. Kullanıcının; sunucu, işletim sistemi, veri depolama alanı üzerinde yönetim işlevi bulunmamaktadır.

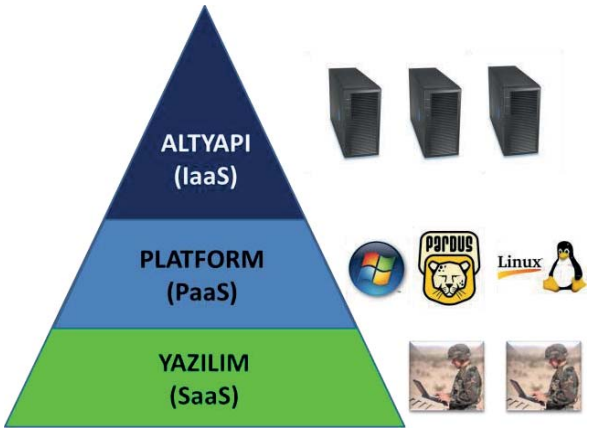
2. Platform Hizmetleri (PaaS - Platform as a Service)

Kullanıcıya kullanabileceği uygulamaları geliştirmesi ve sunabilmesi için uygun servis ortamı sağlanmasıdır. Geliştirilen uygulama ile ilgili alt yapı, ortam ve diğer servisler bulut hizmet sağlayıcı tarafından sağlanır [7]. Kullanıcının işletim sistemi, sunucu, veri depolama alanı üzerinde yönetim işlevi bulunmamaktadır. Kullanıcı ancak geliştirilen uygulamalar üzerinde kontrol sağlayabilmektedir. Bir bulut hizmet sağlayıcısı tarafından (Windows Azure v.b) üzerinde geliştirilen uygulamalarda herhangi bir standartın bulunmaması nedeniyle sadece geliştirilen platform üzerinde kullanılabilmektedir.

3. Altyapı Hizmetleri (IaaS - Infrastructure as a Service)

Bulut sisteminin kaynağı olarak da ifade edilmektedir. Ağ üzerinden güvenli erişim imkânı sunan dinamik veri depolama alanı (Amazon S3 v.b), işlemci kaynaklarının sanal olarak sunulması (Amazon EC2 v.b) ve ağ hizmetleri gibi servisler, bulut sistemi alt yapı servisi örnekleridir. Kullanıcının bulut alt yapısında yönetim işlevi bulunmamaktadır [8]. Fakat işletim sistemi, veri depolama alanı ve sınırlı olarak ağ bileşenleri (güvenlik duvarı gibi) üzerinde kontrol sağlayabilmektedir.

Bulut sistemi hizmetleri tabanını altyapı hizmeti ve bunun üzerine platform ve yazılım hizmetleri gelse de kullanıcı açısında bakıldığında piramit tam tersi şekilde olmaktadır. (Şekil 2).



Şekil 2. Bulut Sistemi Hizmetleri

III. BULUT SİSTEMİNİN ASKERÎ ALANLARDAKİ KULLANIMLARI

Bulut sistemi; karmaşık harekât ortamında taktik resmin oluşturulması için gerekli verilerin güvenilir ve zamanında işlenebilmesi maksadıyla gelişmiş bütün ordu ve askerî organizasyonlar tarafından kullanılmaktadır.

Taktik resim cereyan eden harekâtın istenilen anki fotoğrafıdır. Doğru karar verilmesi için bu fotoğrafta kara, deniz, hava kuvvetleri, insansız hava ve uzay sistemleri, coğrafi bilgi sistem sistemleri, sağlık ve lojistik konularından gelen tüm veriler bulunmak zorundadır (Şekil 3).

Taktik resim oluşturmak için çok fazla veriye ihtiyaç duyulması, bu toplanan verilerin istenen yer ve zamanda hazır bulundurulması gerekliliği bulut sisteminin kullanımını zorunlu kılmaktadır. Ayrıca anlık oluşan ani durumlar ve

rutin faaliyetlerde de bulut sistemi günümüzün olmazsa olmaz bir sistemi haline gelmiştir.

Şekil 3. Taktik resim bileşenleri

IV. Bulut Sisteminin Sağladığı Teknik Faydalar

A. *Erişimde Esneklik*

Bulut sisteminin ana görevi, kullanıcıya ait verilerin ağ üzerindeki bir sunucuya yüklenmesi, depolanması ve gerektiğinde erişilerek bilgiler üzerinde değişikliğin yapılmasını sağlamaktır. Bu nedenle taktik resmin oluşturulmasında mutlaka olması gereken bir sistemdir. Bulut sisteminin en önemli özelliliği her an kullanıcının isteklerine cevap verecek durumda ve yeterlilikte olmasıdır. Bu özelliği ile bulut sistemi, taktik durumun güncellenmesi ve istenen verilere ulaşılabilmesinde en önemli bilgi ve iletişim teknolojileri hizmetlerinden biri haline gelmiştir. Bulut sistemi ile ağ erişimi sağlanabilen her noktadan bilgilere ve uygulama programlarını kullanma imkânına sahip olunabilmektedir. Uzaktan erişim kolaylığı; harekât alanından yapılabilecek bir hırsızlık ya da fiziksel disk problemleri gibi nedenlerle verinin kaybedilme riskini azaltmaktadır.

B. *Kaynak Paylaşımı ve Maliyet*

Bulut sisteminde; kullanıcı sayısı ve sunulan hizmetin niteliğine bağlı olarak maliyetler değişmekte ve yönetilebilmektedir. Hizmet sunmak için kullanılan tüm donanım, bakım ve güncellemeleri hizmet sağlayıcı tarafından yapılmaktadır. Kullanıcı tarafından herhangi bir yazılım ücreti ödenmemektedir. Yazılım maliyeti kullanıcı sayısına bağlı olarak hizmet sağlayıcı tarafından karşılanır. Kullanıcı tarafından veri depolamak için yüksek kapasiteli veri depolama birimlerine ihtiyaç yoktur. Bu sebeple harekâtın hızla geliştiği bir ortamda mobiliteyi artırma adına çok önemli bir hususdur.

C. *Depolama için Kapasite Sınırlamalarının Ortadan Kalkması*

Bulut sisteminde; kullanıcılara tahsisli özel bir disk alanı bulunmamaktadır. Bundan dolayı veri depolama alanının yönetimi daha etkin olarak yapılabilmektedir. Kullanıcılar, depolama alanı kullanımı konusunda, sanal disk üzerinde yazılım ile kısıtlanırlar ve tüm kullanıcılara ait veriler aynı ortamda bulunmaktadır[9]. Kullanıcı bilgisayarında veri depolamak için yüksek kapasiteli veri depolama birimlerine ihtiyaç duyulmamaktadır. Bulut sisteminde kullanılan bilgi ve veri alanı yönetim araçları, eşit seviyede maliyet ile daha geniş veri alanında daha güçlü veri koruma imkânı sunar ki bu husus harekât ortamındaki yoğunluk ve karmaşa düşünüldüğünde en önemli konulardan biridir. Ancak bulut teknolojisinin bu kolaylıklarının yanında bazı risklerde bulunmaktadır. [10]. Bu riskleri üç başlık altında toplayabiliriz:

V. Bulut Sisteminin Oluşturduğu Riskler

A. *Donanım Riskleri*

Bulut teknolojisinde kullanılan alt yapı donanımlarının ve yedeklerinin hasım güçler tarafından imha edilmesi çok ama çok önemli verilerin kaybolmasına ve taktik resmin elde edilememesine neden olabilecektir [11]. Bu durum kolayca onarılamayacak ve olumlu giden bir harekâtın seyrini olumsuz yönde değiştirebilecektir. Bundan dolayı bu alt yapıların fiziki güvenlik risklerinden söz etmek mümkündür. Muharebe esnasında bu sistemlerin çok iyi bir şekilde korunması kesin sonuçlu bir muharebe için şarttır.

B. *Yazılım ve İşletim Sistemleri Riskleri*

Bulut sistemini oluşturan yazılım ve işletim sistemlerinin güvenilir, minimum açıkları olan ve sürekli geliştirilebilir olması çok önemli bir hususdur [12]. Dünyadaki bütün ordu ya da askerî organizasyonlar kendi yazılım ve işletim sistemlerini üretip kullanmaya doğru bir eğilim içerisindedir. Yazılım ve işletim sistemlerinin yanında kriptoloji hususları da veri aktarımında son zamanlarda oldukça önemli ve popüler bir hale gelmiştir.

C. *Kullanıcı Tarafından Oluşturulan Riskler*

Bilinçsiz kullanıcılar tarafından bulut sistemini zayıflatılacak ya da veri kaybına neden olabilecek siber saldırı girişleri yapılmasına müsaade etmesi çok önemli bir risk kategorisidir.

VI. Risklere Karşı Çözüm Önerileri

1) Sistemlerin Milli bir işletim sistemi üzerine inşa edilmesi,
2) Saldırı tespit sistemlerine yönelik milli yazılım ve donanımlar geliştirilmesi ve milli kriptolama sistemlerinin oluşturulması,
3) Operatörlerin ve kullanıcıların bulut sisteme karşı yapılacak saldırılara karşı farkındalığı artırıcı eğitim ve seminerlerin düzenlenmesi,
4) Yine bu kapsamda kurulacak Eğitim Laboratuvar'ları ile kullanıcı ve operatörlerin bir rotasyon dahilinde simülasyon ortamında eğitim ve durum tespitlerinin yapılması,
5) Kullanıcı ve operatörlerin kullandıkları sistemlerde meydana gelebilecek olağandışı tüm olayları uzman personele rapor etmesi,
6) Bulut Sisteminin, yapılacak saldırılardan korunmasına yönelik olarak aynı ünite içerisinde bilgi sistem güvenlik personeli kadroları tesis edilmesi,

7) Periyodik ya da zamansız olarak bilgi sistem güvenlik personeli tarafından öncelikle sistemlerin ve yazılımların, müteakiben kullanıcıların test edilmesini ve bilinçli ya da bilinçsiz olarak sistemin hatalı kullanılımının engellenebilmesi,
8) Sistem alt yapısını oluşturan donanımın bulunduğu bölgelerde emniyet önlemlerinin arttırılması ve yedekleme mekanizmasının çalışmasının uygun olacağı değerlendirilmektedir.

VII. SONUÇ

Harekât Ortamının çok hızlı gelişmesi ve teknolojinin yardımıyla değişmesi bulut teknolojisini zorunlu kılmıştır. Gelişen bu teknoloji ile birlikte risk ve fırsat dengesini göz önüne alarak bulut sisteminin tüm ordu ve askerî organizasyonlarca kriptoloji ile birlikte kullanılması, kullanıcılara etkinlik, maliyet, güvenlik konularında fayda sağlayacağı değerlendirilmektedir.

VIII. KAYNAKLAR

[1] N. Türkay, Bilişim Zemininde Etnik Milliyetçiliğe Dayalı Terörist Faaliyetler, 1st International Symposium on Digital Forensics and Security (ISDFS'13),283.
[2] S.D. Chi, J.S Park, K.C. Jung, and J.S. Lee, Network security modeling and cyber attack simulation methodology. In Information Security and Privacy, pp. 320-333. Springer Berlin Heidelberg, 2001.
[3] A. Lin, N-C. Chen, Cloud computing as an innovation: Percepetion, attitude, and adoption. International Journal of Information Management, , s.533-540.,2012.
[4] T. Henkoğlu, Ö. Külcü, Bilgi Erişim Platformu Olarak Bulut sistemi: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme Cloud Computing as an Information Access Platform: A Study on Threats and Legal Requirements, Bilgi Dünyası, s. 62-86, 2013.
[5] R.Madhubala, An Illustrative study on Cloud Computing, , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, s. 286-290, 2012.
[6] http://www.hakanuzuner.com/index.php/cloud-computing-risk-and-security-assesment-bulut-bilisim-risk-ve-gvenlik-degerlendirmesi.html erişim zamanı: 11.07.2013 23.26.
[7] L. Schubert, The Future Of Cloud Computing: Opportunities for European Cloud Computing, s. 9-11, 2010.
[8] L. Youseff, M. Butrico, D. Da Silva, Toward a unified ontology of cloud computing. In: Grid Computing Environments Workshop, 2008. GCE'08. IEEE, p. 1-10,2008.
[9] T. Velte, A. Velte, R. Elsenpeter, Cloud computing, a practical approach. McGraw-Hill, Inc., 2009.
[10] D. Catteddu, Cloud Computing: benefits, risks and recommendations for information security. Springer Berlin Heidelberg, 2010.
[11] M. Carroll, A. Van Der We, P. Kotze, Secure cloud computing: Benefits, risks and controls. In: Information Security South Africa (ISSA), 2011. IEEE, p. 1-9, 2011.
[12] K. Goztepe, A Study on OS Selection Using ANP Based Choquet Integral in Terms of Cyber Threats. International Journal of Information Security Science, 2012, 1.2: pp.67-78.