Kamusal Bulut Servisleri için Bulanık Mantığa Dayalı Bir Güven Modeli

Mahir Kutay, Tuncay Ercan
Yaşar Üniversitesi, Bilgisayar Mühendisliği Bölümü, İzmir
mahir.kutay@yasar.edu.tr, tuncay.ercan@yasar.edu.tr

Özet: Günümüzde hızla yaygınlaşmakta olan kamusal bulut servislerinin karşılaştığı en büyük sorunlardan biri, kullanıcı ile servis arasındaki güven ilişkisidir. Güven ilişkisini rakamsal sonuçlarla ifade eden ve hizmet sözleşmesine dayalı güven modelleri, bulut servislerinin bileşenleri ve bu bileşenlerin güvenilirliği konularında yetersiz kalmışlardır. Bu çalışmada önerilen bulanık mantığa dayalı güven modeli mevcut eksiklerin büyük ölçüde giderilmesini amaçlamaktadır.

Anahtar Sözcükler: Güven, Bulut Bilişim, Güven Modellenmesi, Bulanık Mantık, Kamusal Bulut.

Fuzzy Logic Based Trust Model for Public Cloud Services

Abstract: Public cloud services are rapidly growing nowadays but they have a big problem to establish a trust relationship between their users. Proposed trust models to describe trust relationship in a formal way are inadequate to describe public cloud components and calculate their trustworthiness. In this research we aim to minimize deficiencies of previous models by developing a fuzzy logic based trust model.

Keywords: Trust, Cloud Computing, Trust Modeling, Fuzzy Logic, Public Cloud

1. Giriş

Bulut bilişim son yıllarda bilgisayar biliminin en hızlı gelişen alanlarından biridir. Internet teknolojisinin gelişmesi ile kuruluşlar bulut servis sağlayıcılarından kiraladıkları kaynaklar ile bilgi-işlem gereksinimlerini hızla karşılamakta ve maliyetlerini önemli ölçüde düşürmektedirler. Bulut servislerinin gördüğü büyük ilgi birçok büyük bilişim şirketini bu alana çekmiştir. Bu şirketler verdikleri düşük maliyetli hizmetler ile çok sayıda küçük organizasyonun ve kişinin servislerinden faydalanmasını sağlamışlardır [1]. Kullanıcılar yapısı ve işleyişi hakkında hiçbir fikirlerinin olmadığı bir kamusal bulut servisine, kendileri için çok önemli olan bilgilerini emanet etmektedirler. Bulut bilişim mevcut bilişim teknoloji güvenlik risklerine ek olarak bilgi güvenliği, ağ güvenliği, kişiye özellik, uyum kuralları, sanal makinaların kullanımı vb. gibi güvenlik riskleri de içermektedir [2].

Ek olarak, bulut servislerinin dağıtık ve saydam olmayan yapısı, güven yönetimini çok daha karmaşık hale getirmektedir [3]. Bu çalışmada bulut servislerinin güven modellenmesinde yetersiz kalan klasik yaklaşımların yerine, kullanıcılardan gelen geri dönüşümleri daha ayrıntılı sınıflayabilen ve belirsiz durumları dikkate alan bulanık mantığa dayalı bir güven modeli geliştirilmiştir.

Makalenin ikinci bölümünde bulut servisleri ile ilgili genel bilgi verilmekte, üçüncü bölümde kullanılmakta olan güven modelleri tanıtılmaktadır. Dördüncü bölümde önerilen model açıklanmış olup sonuç ve gelecekteki çalışmalar beşinci bölümdedir.

2. Bulut Bilişim'e Genel Bakış

Bulut bilişim servislerini kullanıcılar için çekici kılan altyapı, donanım, yazılım lisanslama, personel ve enerji giderleri konusundaki düşük maliyetlerdir. Bulut bilişim servis şirketleri hizmetlerini her biri farklı bir kullanıcı grubuna hitap eden üç farklı seviyede sunar [4]:

- Altyapı (IaaS)
- Platformlar (PaaS)
- Yazılım (Saas)

Bulut bilişim servisleri hizmetin sahipliğine bağlı olarak üç grupta toplanırlar.

- Özel
- Kamusal
- Karmaşık

Özel bulutlar yalnızca bir organizasyonun kullanıcılarına açık, kamuya kapalıdır. Kamusal bulutlarda servis hizmeti internet yoluyla belirli bir kullanıcı grubu hedeflenmeden verilir. Karmaşık bulutlarda ise kaynakların bir kısmı organizasyonun kendi elemanlarına ayrılır, diğer kısmı ise kamuya açıktır [5].

2.1 Bulut Bilişim Servislerinde Karşılaşılan Sorunlar

Maliyetleri azaltma konusunda çok yararlı olan bulut bilişim, servis sağlayıcılar ile bu servislerden yararlanan kişi ve kuruluşlar için bir takım riskleri de beraberinde getirmektedir [6], [7]:

- Bulut bilişim servis sağlayıcılar için en büyük risk verdikleri hizmetin kullanıcılar tarafından kanunsuz ve kötü niyetli amaçlar için kullanılmasıdır.
- Kişi ve kuruluşlar özel bilgilerini bulut' a gönderdikleri veri içinde tutmak zorundadırlar.
- Kullanıcı verisi her zaman servis sağlayıcının yazılımı üzerinden gelebilecek virüs tehditleri altındadır.

2.2 Bulut Bilişim Servislerinde Güvenlik

Bulut servislerinde güvenlik en önemli problemlerden biridir. Güvenliğin sağlanmasında anahtar öneme sahip konular aşağıda ana başlıklarıyla özetlenmiştir [8]:

- Veri güvenliği
- Ağ güvenliği
- Verinin bulunduğu coğrafi yer
- Veri bütünlüğü
- Verinin diğer kullanıcıların verilerinden ayrı tutulması
- Verinin gizliliği
- Kimlik belirleme ve yetki verme
- Web uygulamalarının güvenliği
- Verinin her zaman ulaşılır olması
- Verinin yedeklenmesi

3. Bulut Bilişim Servislerinde Güven

Bulut bilişim servisi sağlayan kuruluşlar verdikleri hizmetin kalitesini sürekli olarak denetlemek zorundadırlar [9]. Kullanıcıların kötü deneyimleri servis sağlayıcılar için kısa sürede büyük maddi kayıplara dönüşebilir.

Servis kalitesinin değerlendirilmesi için en çok kullanılan yöntem geri besleme yöntemidir. Bu yöntemde kullanıcıların aldıkları hizmetler konusundaki değerlendirmeleri web üzerinden toplanır. Kullanıcıların cevaplaması istenilen sorular servis sağlayıcı ve kullanıcı arasında yapılan hizmet sözleşmesi ile uyumlu olmalıdır [10].

3.1 Hizmet Sözleşmesine Dayalı Güven Modeli

Hizmet sözleşmesi servis sağlayıcının kullanıcıya önerdiği hizmetin ayrıntılarının yasal bir biçimde yazıya dökülmesidir. Kullanıcı kendisine güvence verilen hizmet kalitesi ile gerçekte almış olduğu hizmeti karşılaştırarak servis sağlayıcıya web üzerinden değerlendirme bilgilerini gönderir. Servis sağlayıcı bu bilgileri analiz ederek kullanıcıların hizmetten ne kadar memnun kaldıklarını ölçebilir. Elde edilen sonuçlar kullanıcının servis sağlayıcıya duyduğu güvenin bir ölçüsüdür. Bu yöntemin başarılı

olabilmesi için aşağıda belirtilen özelliklere sahip olması gereklidir [11].

- Kullanıcıların gereksinimlerine göre sınıflandırılması.
- Kullanıcıya sorulacak geri besleme sorularının kullanıcının beklentilerine göre hazırlanması
- Geri besleme bilgisinin kullanıcının hizmeti alma sıklığına göre belirlenmesi.
- Toplanan geri besleme bilgisinin değerlendirilerek hizmet kalitesinin zaman içindeki değişiminin belirlenmesi.

Güven modelinin başarısı önemli ölçüde bilginin değerlendirilmesi yöntemlerine bağlıdır.

3.2 Verilerin Analizi

Önerilen modeller arasındaki fark toplanan geri dönüşüm bilgisinin işlenme yöntemine bağlıdır. Birçok araştırmacı modellemeyi öznel mantık ve istatistiksel yöntemlere dayandırmışlardır [12], [13], [14]. Bu modellerin en büyük eksikliği elde edilen matematiksel sonuçların kullanıcılar için yeterince anlaşılır olmaması ve belirsiz değerler için doğru sonuçlara ulaşılamamasıdır [15]. Bu araştırmamızda önerdiğimiz bulanık mantığa dayalı model sonuçları semantik olarak kullanıcı ve servis sağlayıcıya aktarır. Sonuçların kolay anlaşılır olması tarafların karalarını kolaylıkla ve hızlı alabilmelerine yardımcı olur.

4. Önerilen Model

Modelimiz yalnızca kamusal bulut servislerini kapsar. Bu nedenle kullanıcılarımızı bireyler ve küçük kuruluşlar oluştur. Kullanıcılar özne kümesi U'nun elemanlarıdır. Nesnemiz içerik kümesi V dir. U kümesinin elemanları V kümesinin elemanlarına elemanlarına bir m_t bulanık üyelik fonksiyonu ile bağlıdırlar. U nun bulanık alt kümeleri $T_1, T_2, ..., T_k$ U'nun bir elemanının bir içerik için verdiği bulanık fonksiyon değerini gösterir. Örneğin, bir kullanıcı kamusal servis sağlayıcı ile dört maddelik bir hizmet sözleşmesi imzalamış olsun. Bu maddelerin;

- Güvenlik
- Veri gizliliği
- Hizmetin kesintisiz olarak devam etmesi
- İşlem hızı

konularını kapsadığını varsayalım. Kullanıcıların verdikleri sözel cevaplar aşağıdaki gibi seçilebilir.

- Çok kötü
- Kötü
- Orta
- İyi
- Çok iyi

Verilen cevaplar aşağıdaki bulanık alt kümelere bağlanırlar. Bu alt kümelerin her biri bir güven aralığını temsil eder.

- Çok kötü---[0,0.10]
- Kötü--------[0.10,0.45]
- Orta-------- [0.45,0.55]
- İyi----------[0.55,0.90]
- Çok iyi------[0.90,1]

4.1 Kullanıcıların Servis Sağlayıcıya Genel Güveninin Hesaplanması

Özne kümemiz U yalnızca kamusal kullanıcılardan oluştuğundan kullanıcılar alt kümelere bölünmemişlerdir. Her bir içerik için $[t_1, t_2]$ zaman aralığındaki güven değerinin hesabı aşağıda verilmiştir.

$m_1, m_2, ..., m_k$ bulanık değerlendirme kümelerinin ortalama değerleridir. Yukarıda verilen örnekte bu değerler.

$$m_1 = 0.050$$

$$m_2 = 0.275$$

$$m_3 = 0.500$$

$m_4 = 0.725$

$m_5 = 0.950$

Her bir içerik için değerlendirme yapanların sayısı $n_1, n_2, ..., n_k$ olsun. Her bir içeriğin toplam güven içindeki ağırlığı:

$$w_{tk} = \frac{n_k}{\sum_{i=1}^{k} n_k}$$

Toplam güven değerimiz:

$$T_{total} = \sum_{i=1}^{k} w_{tk} \times m_i$$

Örneğin :

$w_{t1} = 0.30$

$w_{t2} = 0.15$

$w_{t3} = 0.20$

$w_{t4} = 0.20$

$w_{t5} = 0.15$ ise

$T_{total} = 0.5745$ bulunur ki bu da, kullanıcıların servis sağlayıcıya olan güveninin iyi olduğunu gösterir.

5. Sonuç ve Gelecek Çalışmalar

Bu araştırmamızda, olasılıksal mantık kullanan bulut güven modellerinin belirsizlik durumlarını ortadan kaldıran ve kullanıcı ve servis sağlayıcıya kolay anlaşılır sözel sonuçlar veren bir model geliştirdik. Şu anda yalnızca kamusal bulut servis sağlayıcılarını hedefleyen modelimizin özel ve karmaşık bulut modellerini de kapsayacak sekilde geliştirilmesine çalışılmaktadır. Ayrıca web üzerinden toplanan kullanıcı geri besleme bilgilerinden modelimizi kullanarak güven değerlerini hesaplayan CTRUST adını verdiğimiz PHP tabanlı bir yazılım üzerinde çalışmaktayız.

6. Kaynaklar

[1] Ahmed, M., Chowdhury, R., Ahmed, M. and Rafee, M., H., "An Advanced Survey on Cloud Computing and State-of-the-art Research Issues", International Journal of Computer Science Issues, Vo.9, Issue 1, No.1, (2012).

[2] Agrawal, A., "The Security Riscs Associated with Cloud Computing", International Journal of Computer Applications in Engineering Sciences, Vol.1, Special Issue on CNS, (2011).

[3] Noor, T., H., Sheng, Q., Z., Zeadally, S., Yu, "Trust Management of Services in Cloud Environments: Obstacles and Solutions", ACM Computing Surveys, Vol.46, Issue 1, (2013).

[4] Patidar, S, Rane, D., Jin, P., "A Survey Paper on Cloud Computing", Second International Conference on Advanced Computing and Communication Technologies, (2012).

[5] Zhou, M., Zhang, R., Zeng, D., Quian, W., "Services in the Cloud Computig Era: A Survey", 4th International IUCS Conf., pp. 40-46, (2010).

[6] Harauz, J., Kaufmann, L., M., Potter, B., "Data Security in the World of Cloud Computing", Journal of IEEE Security and Privacy, July/August, pp.61-64, (2009)

[7] Takabi, H., and Joshi, J., "Security and Privacy Challenges in Cloud Computing Enviromments", Journal of IEEE Security and Privacy, November/ December, pp.24-31, (2010).

[8] Subashini, S., Kavitha, V., "A Survey on Security Issues in Service Delivery Models of Cloud Computing", Journal of Computer and Network Applications, No.34, pp.1-11, (2011).

[9] Khan, K., M., and Malluhi, Q., "Establishing Trust in Cloud Computing", Journal of IT Professional, Vol.12, No.5, pp.20-27, (2010).

[10] Alhamad, M., Dillon, T., Chang, E., "Sla Based Trust Model for Cloud Computing", 13th International Conference on Network Based Information Systems, (2010).

[11] Li, X., and Du., Ju, "Adaptive and Attribute-Based Trust Model for Service-Level Agreement Guarantee in Cloud Computing", Journal of IET Information Security, Vol.7, No.1, pp.39-50, (2013).

[12] Wu, X., Zhang, R., Zeng, B., Zhou, S., "A Trust Evulation Model for Trust Computing", Procedia Computer Science, No.17, pp.1170-1177, (2013).

[13] Firdhous, M., Ghazali, O., Hassan, S., "Trust Management in Cloud Computing: A Critical Review", International Journal on Advances in ICT for Emerging Regions, Vol.4, No.2, pp.24-36, (2011).

[14] Pawar, P., S., Rajarajan, M., Nair, S., K., Zisman, A., "Trust Model Optimized for Cloud Services", IFIP Advances in Information and Communication Technology, No.374, pp.97-112, (2012).

[15] Nafi, J.J., Liker, K.W., Kar, S., and Hashem, M.M.A., "A Fuzzy Logic Based Certain Trust Model for E-Commerce", Proceedings of the IEEE International Conference, Electronics and Vision, (2013).