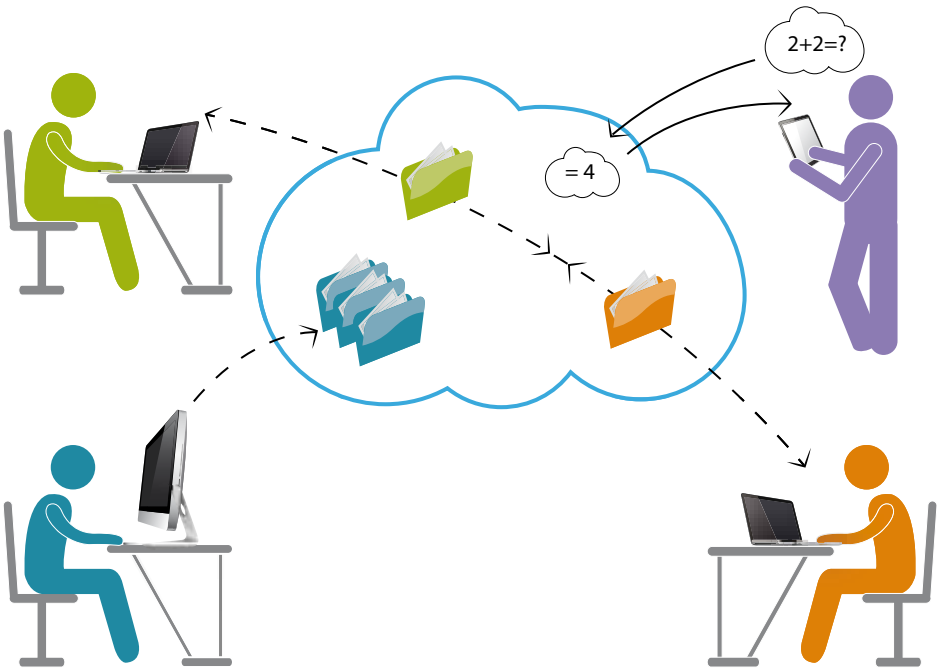
Gelecek Nesil Bulut Sistemleri için Yüksek Performanslı Kriptolojik Çözümler

Sanal Varlığınızı Güvence Altına Alın!

Yar. Doç. Dr. Alptekin Küpçü Koç Üniversitesi Bilgisayar Bilimi ve Mühendisliği



Koç Üniversitesi Kriptoloji, Güvenlik ve Gizlilik Araştırma Gurubu küresel sorunlara yüksek performanslı ve tamamen güvenli çözümler hazırlıyor.

Bulut bilişimin bize depolama, hesaplama ve dağıtım alanlarında sunduğu sınırsız seçeneklerden hepimiz yararlanıyoruz. Örneğin, Dropbox ve Wuala gibi bulut depolama sistemleri verilerimize istediğimiz zaman istediğimiz yerden erişebilmemizi sağlıyor. Amazon EC2 ve SETI@Home projeleri ise bizim cihazlarımızın kapasitesini aşan hesaplama işlerini taşeronlara yaptırabilmemize olanak tanıyor. Bu sayede gerek güçlü bilgisayarlar gerekse pek çok ufak bilgisayar kullanılarak sorun çözülebiliyor. Rapidshare ve BitTorrent ise kendi bilgisayarlarımızın kapasitesini zorlamadan dosyalarımızı arkadaşlarımızla veya dünya ile kolayca paylaşmamızı ve dağıtmamızı sağlıyor. Ancak şu anki bulut çözümlerinin hepsi beraberinde çeşitli riskler de getiriyor.

Dropbox, Sugarsync, Box, Google Drive veya benzeri bir servis kullanıyor musunuz? Eğer kullanıyorsanız, bu şirketlerin verilerinizin kaybı ya da değiştirilmesi durumlarında hiçbir sorumluluk kabul etmediklerinin farkında mısınız? Ne yazıktır ki günümüzdeki bulut depolama sistemlerinin hiçbiri verinizin değiştirilmeden, aynen saklanacağı konusunda kanıtlanabilir bir garanti sunmuyor. Güzel haber şu ki, kriptolojik teknikler kullanarak verinizin aynen korunup korunmadığına dair sunucudan bir kanıt istemek mümkün.

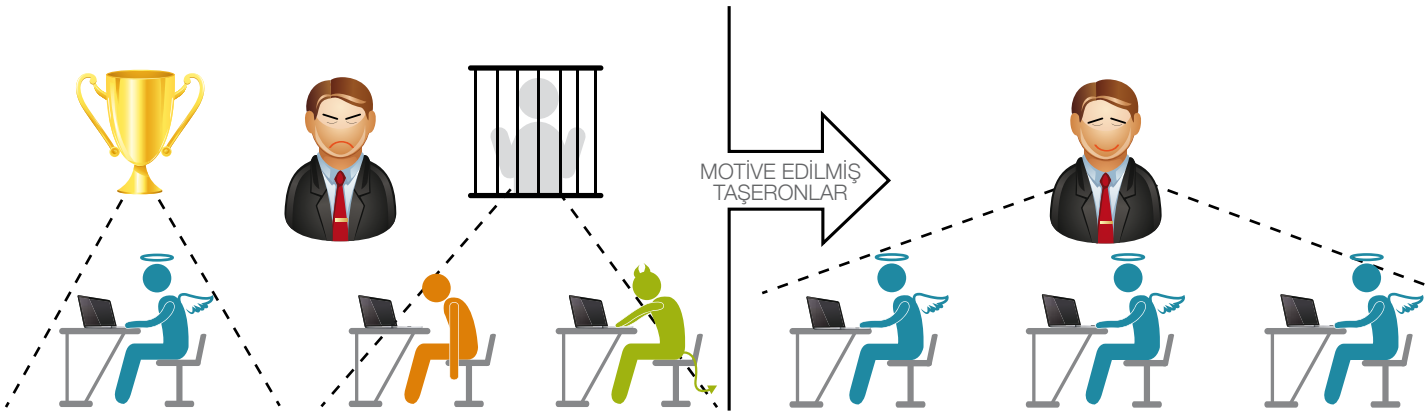
Gurubumuz var olan bulut sistemlerindeki sorunlara yüksek performanslı kriptolojik çözümler getirerek gelecek nesil bulut sistemlerinin daha tasarım aşamasında kanıtlanabilir seviyede bir güvenliğe sahip olmasını sağlıyor.

Bizim güvenli bulut depolama sistemimiz buluta koyduğunuz verinizle ilgili çok ufak bir bilgiyi yerel olarak bilgisayarınızda tutuyor. Bu bilgiyi kullanarak isterseniz buluttaki verilerinizi güncelleyebilir ve karşılığında güncellenmiş bir yerel veriye sahip olabilirsiniz. Daha sonra istediğiniz bir zaman depolama sunucusundan verinizin aynen korunduğunu ispatlamasını isteyebilirsiniz. Eğer sunucunun yolladığı kriptografik ispat elinizdeki yerel veriye göre geçerli değilse dosyalarınız değiştirilmiş ya da silinmiş demektir. Bu durumda resmi bir mahkemede hakime başvurup bir garanti ödemesi talep edebilirsiniz. Hatta mahkeme kapılarında sıra beklemenize bile gerek yok: Hakim olarak yalnızca bir bilgisayar kullanmak ve ödemeleri elektronik ortamda gerçekleştirmek de mümkün. Bu proje kısmen Türk Telekom ve Koç Sistem tarafından desteklenmektedir. Bu da demektir ki şu aşamada kriptolojik kütüphanemizi kullanarak ön kodlamasını gerçekleştirdiğimiz bu sistemin yakın zamanda halka açılması olası ve böylece insanların hayatlarını değiştirmek elinizde.

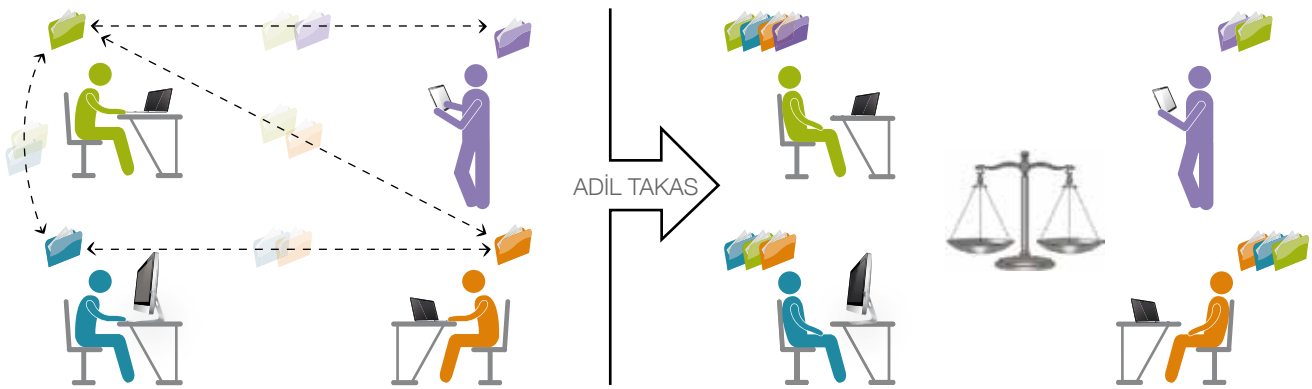
Hiç SETI@Home, Folding@Home veya Electric Sheep gibi bir bulut bilişim projesinde taşeron olarak yer aldınız mı? Aldıysanız bu tür sistemlere sahte yanıtlar göndererek taşeronlar listesindeki ününüzü artırmaya çalıştınız mı? O listede en üstteki kullanıcıların nasıl o seviyelere geldiklerini hiç merak ettiniz mi? Yine üzülerek belirtmek durumundayız ki şu anki taşeron hesaplama sistemlerinin hiçbirinde taşeronların verdiği sonuçların doğruluğunu garantileyen bir mekanizma yok. Ancak, kriptoloji ile birlikte oyun teorisi ve mekanizma tasarımı tekniklerini kullanarak ortaya çıkardığımız sistem ile hilekar taşeronlar olduğunda bile sonuçların doğruluğunu çok yüksek düzeyde garantilemek mümkün.

Zaman zaman hepimiz patron olmak isteriz; işlerimizi taşeronlara yaptırmak isteyebiliriz. Elbette ki böyle bir durumda taşeronların işi doğru düzgün yapmalarını isteyeceksiniz. Var olan sistemler bu garantiyi sunmadığı için bizim sistemimizi kullanmaya karar veriyorsunuz. Bizim taşeron hesaplama sistemimizin parametrelerini ayarladığınızda sonuçların doğruluk garantisine siz karar veriyorsunuz; %99 doğruluk mu istersiniz, %99,9 mu, yoksa daha fazla mı, size kalmış. Ayrıca, sistemimiz dürüst taşeronları ödüllendirmenize ve hilekar taşeronları cezalandırmanıza da imkan sunuyor.

Hiç BitTorrent, Kazaa veya Napster kullanarak bir dosya indirdiniz mi? İndirir indirmez paylaşımınızı sonlandırıyorsunuz, değil mi? Aslında bu tür sistemlerde mümkün olandan daha yavaş bir hızda dosya indiriyor olmanızın bir sebebi de herkesin aynı şeyi yapıyor olması. Beleşçi olarak adlandırdığımız ve içinde bulunduğumuz bu gurup, sistemden kendi istediklerini aldıkları anda sisteme katkıda bulunma-



Kriptoloji hayal bile edemeyeceğiniz şeyleri gerçekleştirir...



yı kesiyor. Yalnızca az sayıda yardımsever kullanıcı sistemden bir beklentisi olmadan sisteme katkıda bulunmaya devam ediyor. Ama kriptolojik adil takas teknikleri kullanarak herkesin sistemden aldığı kadar sisteme katkıda bulunmasını garantilemek ve böylece sistem genelinde katılımı artırarak performansı üst seviyelere taşımak mümkün.

Bir adil takas Aliye ve Bora diye adlandırdığımız iki tarafın birbirleriyle birer eşya (ör: dosya) değişmek istemesiyle ortaya çıkar. Burada adalet ile kastımız şudur: Ya hem Aliye Bora'nın dosyasını hem de Bora Aliye'nin dosyasını elde edecek, ya da iki taraf da sonuçta bir şey elde etmemiş olacak. BitTorrent dosya paylaşım sistemi üzerine adil takas protokolünü uygulamak demek, bir dosya indirebilmek için sisteme bir dosya göndererek katkıda bulunmanın gerekmesi demektir. Böylece beleşçi sorunu ortadan kalkacak, herkes sisteme sistemden kazandığı ölçüde katkıda bulunacak ve sistemin toplamdaki performansı kat kat artacaktır. Ayrıca adil takas fikri yalnızca BitTorrent ile sınırlı değildir. Eğer internetin adil bir ortam olması gerektiğini düşünüyorsanız TÜBİTAK destekli "İnternette Eşitlik ve Adalet" isimli projemize katılarak adalet fikrini çeşitli diğer internet sistemlerine, örneğin bulut bilişim ve depolama sistemlerine, uygulama şansını yakalayabilirsiniz.

Eğer Koç Üniversitesi Kriptoloji, Güvenlik ve Gizlilik Araştırma Gurubu'na katılırsanız olanaksız gözüken bir gerçekliğin yepyeni dünyasına yelken açarsınız. Kriptoloji hayal bile edemeyeceğiniz şeyleri gerçekleştirir...

Kaynakça:
[Kitap] Alptekin Küpçü. "Efficient Cryptography for the Next Generation Secure Cloud: Protocols, Proofs, and Implementation". Lambert Academic Publishing, 2010.
[BulutDepolama] Chris Erway, Alptekin Küpçü, Charalampos Papamanthou and Roberto Tamassia. "Dynamic Provable Data Possession". ACM CCS bildiri kitapçığında, 2009.
[BulutBilişim] Mira Belenkiy, Melissa Chase, Chris Erway, John Jannotti, Alptekin Küpçü and Anna Lysyanskaya. "Incentivizing Outsourced Computation". Network Economics bildiri kitapçığında, 2008.
[AdilTakas] Alptekin Küpçü and Anna Lysyanskaya. "Usable Optimistic Fair Exchange". Computer Networks, 2012, sayı 56, sayfa 50-63.
[Kütüphane] Sarah Meiklejohn, Chris Erway, Alptekin Küpçü, Theodora Hinkle and Anna Lysyanskaya. "ZKPDL: Enabling Efficient Implementation of Zero-Knowledge Proofs and Electronic Cash". USENIX Security bildiri kitapçığında, 2010. http://github.com/brownie/cashlib

Alptekin Küpçü 2010 yılında Brown Üniversitesi Bilgisayar Bilimi Bölümü'nden doktora derecesiyle mezun oldu. O zamandan beri Koç Üniversitesi Mühendislik Fakültesi'nde yardımcı doçent olarak çalışmakta ve kurduğu Kriptoloji, Güvenlik ve Gizlilik Araştırma Gurubu'nu yönetmektedir. Araştırma odağı olarak uygulamalı kriptoloji ve bunun bulut sistemleri güvenliği, gizlilik, görevdeş ağlar ve mekanizma tasarımı ile olan kesişimleri belirtilebilir. Çeşitli patent başvuruları ve ödülleri bulunmakla birlikte geçtiğimiz 2 sene içerisinde çeşitli kaynaklarca desteklenen 6 araştırma projesinde yer almış, bunların 4 tanesini kendisi yönetmiştir. Daha fazla bilgi için: http://crypto.ku.edu.tr