Ek_A1

University	:	**Istanbul Technical University**
Institute	:	**Informatics Institute**
Science Programme	:	**Computer Science**
Programme	:	**Computer Science**
Supervisor	:	**Prof. Dr. Ali Emre HARMANCI**
Degree Awarded and Date	:	**PhD – October 2015**

ABSTRACT

SECURE PLATFORM AS A SERVICE CLOUD DESIGN

Mehmet Tahir SANDIKKAYA

This doctoral study is aimed to design a secure Platform-as-a-Service cloud design. Previous studies are shown that security is the most important defect of clouds. Moreover, security is counted as the primary concern of prospective customers as well as draws a vastful of attention from academic world.

During the design, the thesis brings solutions to the many aspects of the security of the cloud. If the proposed solutions are deficient in some sense, this is noted right after the security solution is proposed in the text.

The first chapter defines and introduces the cloud.

The second chapter explains the evolution and development of the cloud as well as discusses the coverage of security in the cloud and defines the outline of the thesis.

The third chapter is an attempt to fix the common security problems of concurrent Platform-as-a-Service clouds. Currently deployed Platform-as-a-Service clouds provide computational power by threads. Isolation of threads is the main concern of security in this kind of clouds to not to interfere the date of distinct bodies that use the cloud. Better ways of isolating threads is sought and limits of isolation are shown in the third chapter.

A secure Platform-as-a-Service cloud is designed based on the main proposition of the fourth chapter, which is providing computational power by processes is more convenient and easier than threads. Possible problems and solutions to these problems are enlisted. The design has two flaws. First, it is not clear how to run processes in the cloud within their context. Second, an undeniable and fair logging mechanism does not exist to record events occurred in the cloud. The design is enhanced with novel mechanism to fix these issues. Each of these is explained separately in its own chapter.

In the fifth chapter, methods of securely executing the processes in the cloud are explained. Execution and isolation of processes in the cloud as well as management access control and permissions to the cloud resources are issues that are integrated in process containers. Cryptologic measures to adopt these issues are also covered within process containers in this chapter.

In the sixth chapter, a mechanism where the service providing party and the service user in the cloud are treated fairly is introduced. In this mechanism occurred events are neutrally and undeniably recorded to logs. This is an alternative to problematic conventional logging mechanisms in which only one of the parties is controlling the records. The proposed mechanism may ease to solve the potential conflicts in between the parties.

The presented design discusses all of the defined aspects of the security of a Platform-as-a-Service cloud and proposes solutions to them.

Ek_A2

Üniversitesi	:	**İstanbul Teknik Üniversitesi**
Enstitüsü	:	**Bilişim Enstitüsü**
Anabilim Dalı	:	**Bilgisayar Bilimleri**
Programı	:	**Bilgisayar Bilimleri**
Tez Danışmanı	:	**Prof. Dr. Ali Emre HARMANCI**
Tez Türü ve Tarihi	:	**Doktora – Ekim 2015**

ÖZET

GÜVENLİ HESAPLAMA ORTAMI SUNAN BULUT TASARIMI

Mehmet Tahir SANDIKKAYA

Tez çalışmalarına güvenli bir hesaplama ortamı sunan bulut tasarımı oluşturmak amacıyla başlanmıştır. Öncül çalışmalar bulutun hem en önemli eksiğinin hem müşterileri bulutu kullanmaktan alıkoyanın hem de akademik olarak en çok ilgi çeken konunun güvenlik olduğunu ortaya koymaktadır.

Tasarım sırasında tezin bölümleri bir bütünlük içinde hesaplama ortamı sunan bulutların farklı güvenlik sorunlarını belirleyerek ve irdeleyerek sayılan tüm sorunlara çözüm önerileri getirir. Önerilen çözümlerin bilinen kısıtları ya da eksikleri varsa bunlar çözümün açıklanmasının hemen ardından belirtilmiştir.

Tezin birinci bölümü bulutun tanımını ve tanıtımını yapar.

İkinci bölüm bulutun tarihsel evrimini ve gelişimini açıkladıktan sonra güvenlik tartışmasının kapsamını belirler ve tezin sınırlarını çizer.

Üçüncü bölüm günümüzde sık kullanılan hesaplama ortamı sunan bulutların güvenlik gereksinimlerinin giderilmesine yönelik bir girişimdir. Günümüzde kurulu hesaplama ortamı sunan bulutlar hesaplama gücünü çoğunlukla izlekler yoluyla sunar. Bu tür bulutlarda hesaplama yapanların verilerinin birbirine karışmaması için izleklerin yalıtımı güvenliğin temelini oluşturur. İzleklerin daha iyi yalıtılması yolları üçüncü bölümde araştırılmış, yalıtımın sınırları gösterilmiştir.

Dördüncü bölümde izleklerden daha güvenli ve kolay biçimde hesaplama gücünü sunmanın bir yolu olarak süreçlerin kullanılması önerilerek bir güvenli hesaplama ortamı sunan bulut tasarımı yapılır. Olası sorunlar ve çözümler sıralanır. Tasarımın açıkta kalan noktaları vardır. Bunlardan biri süreçlerin bağlamlarıyla birlikte bulutta nasıl yönetileceği, diğeri de bulutta gerçekleşen olayların tarafsız ve yadsınamaz biçimde nasıl günlüklere aktarılacağıdır. Bu konular için yenilikçi yaklaşımlarla tasarım genişletilir ve her biri kendi bölümünde ayrıca açıklanır.

Beşinci bölümde süreçlerin bulutta güvenli biçimde çalıştırılmaları için nasıl bir yol izlenmesi gerektiği açıklanır. Süreçlerin bulutta çalıştırılmaları, yalıtımları, erişim kurallarının ve buluttaki kaynakların kullanımının yönetimi, bu sırada alınması gereken kriptolojik önlemleri bir arada içeren süreç kozaları bu bölümün konusudur.

Altıncı bölümde bulutu kullanan taraf ile bulutta hizmet sağlayan tarafın eşit sayılarak bulutta gerçekleşen olayların tarafsız ve yadsınamaz biçimde günlük kayıtlarına aktarıldığı, biçimsel olarak doğrulanmış bir düzenek tanıtılır. Bu düzenek kurulu bulutlarda önemli bir sorun oluşturan tek tarafın denetimindeki günlüklere bir seçenek oluşturur ve kayıtlara karşın çözülemeyen uyuşmazlıkların ortadan kalkmasında yararı olacağı düşünülmektedir.

Yapılan tasarım, hesaplama ortamı sunan bulutun güvenliğini belirlenen çerçeve içinde tüm yönleriyle tartışmış ve sayılan güvenlik zayıflıkları için önlemler getirmiştir.