Bulut Tabanlı Donanım Güvenlik Modülü İncelemesi

BİL 420 / 520 Siber Güvenliğe Giriş Proje Raporu

Muhammed Said Zengin
Bilgisayar Mühendisliği
Tezli Yüksek Lisans
muhammedsaid.zengin@etu.edu.tr
201111019

Berk Utku Yenisey
Bilgisayar Mühendisliği
Tezli Yüksek Lisans
b.yenisey@etu.edu.tr
201111010

***Özet*—Bu çalışmada, bulut tabanlı donanım güvenlik modülleri incelenmiş ve bu modülü sunan firmalar araştırılmıştır. Fiziksel olarak kullanılan donanım güvenlik modülleri ile bulut tabanlı modüller karşılaştırılmıştır. Olası saldırılar ve zafiyetler incelenmiştir. Bu modüllerin zaman, güvenlik ve maliyet gibi parametreleri incelenmiştir. Bu sistemlerin Türkiye'deki kullanım alanları araştırılmış, bu sistemleri kullanımının önündeki engeller çıkarılmış ve kullanmak için yapılacak gerekli düzenlemeler önerilmiştir.**

***Anahtar Kelimeler*—hsm, cloud, cloud hsm, security, key**

I. Giriş

İnsanlık antik çağlardan itibaren gizli ve önemli bilgilerin taşınması esnasında bu bilgileri saklama ihtiyacı duymuştur. Sezar şifrelemesinden Enigma'ya kadar yapılan yüzlerce çalışma kriptografinin hikayesinde önemli rol oynamaktadır. Günümüzde kriptografi hayatımızın her alanında önemli bir ihtiyaç haline gelmiştir. Teknolojinin ve bilimin gelişmesiyle birlikte dijital imzalar, kripto paralar, şifreleme standartları, şifreleme anahtarları biz farkında olmasak da aslında sürekli olarak kullandığımız araçlar haline gelmiştir. Hassas verileri korumak, güvenli iletişimi sağlamak, iletişimin doğruluğunu, bütünlüğünü ve gizliliğini korumak için bu konudaki araştırmalar sürekli olarak devam etmektedir.

Donanım güvenlik modülleri güçlü kimlik doğrulama için gerekli sayısal anahtarları koruyup yöneten fiziksel bir aygıttır. Bu modüller bilgisayarlara entegre edilebilen harici fiziksel aygıtlardır. İşlemleri kayıt altında tutar, yetkisiz erişim denemelerini engeller ve gerekli durumlarda anahtarları silerler. Donanım güvenlik modüllerinin güvenlik seviyeleri için uluslararası düzeyde çeşitli standartlar oluşturulmuştur ve donanım güvenlik modülleri bu standartlara göre tasdiklenirler.

Donanım güvenlik modülleri açık anahtar şifreleme kullanılan ortamlarda, sertifikasyon yetkilendirmesi ve kayıt yetkilendirmesi tarafından anahtar çiftlerini oluşturmak, depolamak ve işlemek için kullanılabilir. Bazı modüller kartlı ödeme sistemlerinde kullanılırken bazıları SSL bağlantısında da kullanılmaktadır. Normal bir donanım güvenlik modülü saniyede 50 ile 1000 arasında 1024 bitlik RSA işlemi yapabilmektedir. Bu iş için özelleştirilmiş modüller ise saniyede yaklaşık 7000 işlem yapabilmektedir.

Donanım güvenlik modülleri son yıllarda bulut tabanlı sistemlerde sunulmaktadır. Amazon, Google, Microsoft, IBM gibi firmalar bu hizmeti kullanıcılarına sunmaktadır. Uluslararası standartlara uyumlu olarak hazırlanmış ve kullanıcılara belirli ücret karşılığında sunulan hizmet sistemler hazırlanmıştır. Bulut tabanlı donanım güvenlik modülü sistemleri donanım tedarik etme, yazılım düzeltme eki uygulama, yüksek erişilebilirlik ve yedeklemeler gibi zaman alan yönetim görevlerini otomatikleştiren sistemlerdir.

II. Donanım Güvenlik Modülleri

Kimlik doğrulama için kullanılan sayısal anahtarların yönetimini ve korunmasına yarayan fiziksel aygıta donanım güvenlik modülü denir.[1] Çoğunlukla donanım güvenlik modülleri, bilgisayarların işletim sistemleri içerisinde gömülü olarak saklanan ya da harici bir şekilde tutulan anahtarların yedeklenmesini amaçlar. Kullanıcılara güven vermek hedefi ile bu modüller, Common Criteria ya da FIPS 140 gibi uluslararası standartlara uygun olarak sertifikalandırılmıştır. Güvenlik donanım modülleri, güvenli kriptografik anahtar üretimi, anahtar yönetimi, anahtar yedekleme ve dijital imza fonksiyonları gibi önemli sayıda alanda kullanılmaktadırlar. Özelleştirilmiş banka donanım güvenlik modülleri, kart işlem sistemlerinde yetkilendirme ve kişiselleştirme için kullanılırken, kripto paraların saklandığı kripto cüzdanlar ise özelleştirilmiş donanım güvenlik modülleri üzerinde saklanmaktadır.

THALES Safenet Luna HSM 7 [13]

III. Bulut Tabanlı Donanım Güvenlik Modülleri

Bulut tabanlı donanım güvenlik modülü, şifreleme anahtarlarının barındırılmasına ve FIPS 140-2 Düzey 3 sertifikalı donanım güvenlik modüllerinden oluşan bir kümede kriptografik işlemler gerçekleştirilmesine imkan sağlayan, bulutta barındırılan donanım güvenlik modüllerine denir.[2]

A. AMAZON AWS CloudHSM

Bulut tabanlı bir güvenlik modülü olan AWS CloudHSM kullanıcıların AWS Cloud üzerinde kendi şifreleme anahtarlarını oluşturmasına ve kullanmasına olanak sağlar. FIPS 140-2 Seviye 3 olarak doğrulanmış olan AWS CloudHSM ile kullanıcılar anahtar yönetimini yapabilirler. CloudHSM sayesinde kullanıcılar yedekleme, yazılım düzeltme eki, yüksek kullanılabilirlik ve donanım sağlama gibi önemli ölçüde zaman alan görevleri otomatikleştirebilirler. [3]

AWS CloudHSM kullanıcıların HSM'lerini Amazon EC2 bulut sunucuları üzerinde çalışan uygulamalarla kullanılabilmesini sağlarken kullanıcıların Amazon Virtual Private Cloud 'ları (VPC) üzerinde çalışır. Kullanıcıların uygulamaları, HSM istemci yazılımı tarafından oluşturulan karşılıklı olarak doğrulanmış SSL kanalları üzerinden kullanıcıların HSM'lerine bağlantı kurar.

- AWS, kullanıcının anahtarlarına erişime sahip olmadan donanım güvenlik modülü (HSM) aracını yönetir.
- Kullanıcılar kendi anahtarlarını yönetir ve kontrol ederler.
- AWS iş yüklerine olan yakınlık nedeniyle uygulama performansı iyileşir.
- Kurcalamaya dayanıklı donanımda güvenli anahtar depolaması, birden çok erişilebilirlik alanında sunulur.
- Kullanıcıların HSM'leri diğer AWS ağlarından izole edilmiş bir şekilde sanal özel bulutlarında (VPC) bulunur.

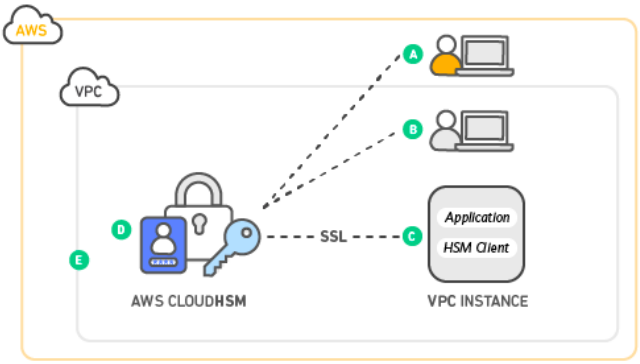

Fig. 1. AWS Cloud HSM

- Amazon CloudHSM Kullanım Senaryoları:
Web sunucuları için SSL işleminin boşaltılması:

- Web sunucularının kimliğini onaylamak ve internet üzerinden güvenli HTTPS bağlantıları kurabilmek için SSL ve TLS kullanılır.
- SSL/TLS işlemlerinin web sunucusu üzerindeki yükü azaltmak için AWS CloudHSM kullanılabilir.
- Web sunucularının özel anahtarlarının AWS CloudHSM üzerinde saklanması ekstra güvenlik sağlar.

Özel anahtarların düzenleyen sertifika yetkilisinden (CA) korunması:

- Sertifika yetkilisi ortak anahtar altyapısında (PKI), bir kişi veya kuruluşu tanımlamayı sağlayan dijital sertifikaları, yayınlayan güvenilir bir varlıktır.
- AWS CloudHSM özel anahtarların depolanması ve sertifika isteklerinin imzalanması için kullanılabilir. Bu sayede AWS CloudHSM kullanan kuruluşlar kendi dijital sertifikalarını kendileri düzenleyerek güvenli şekilde hareket edebilirler.

B. THALES Luna CloudHSM

Anahtar kasaları, kriptografik anahtarları ve sırları korumak için kullanılan güvenli ve güvenilir mekanizmalardır. Kullanıcılar anahtar kasalarını kullandıkları hizmetler ve uygulamalar arasında ortak bir güven dayanağı oluşturarak şifreleme anahtarları oluşturmak ve / veya depolamak için kullanabilirler. Luna CloudHSM ise önemli sayıda kullanım senaryosu bulunan jenerik bir anahtar kasasıdır. [4]

Luna CloudHSM'in Ana Özellikleri:

- Genişletilmiş Denetim özellikleri
- Uyumluluğu sağlamak için politikalar tasarlama ve uygulama becerisi
- Kullanıcıların anahtarlarının desteklenen uygulamalar genelinde yönetebilmesine olanak tanınması
- Anahtar oluşturmak için bir kullanıcı arayüzü ve hizmet katmanı (GUI / API)

Luna CloudHSM Kullanmanın Kullanıcılara Faydaları:

- Kullanıcı verilerinin korunması
- İhtiyaç duyulan anahtar güvenlik politikalarının uygulanmasının sağlanması
- Temel denetim yeteneklerinin sağlanması
- Yöneticinin üzerindeki denetim sorumluluğu ve yükünün azaltılması

C. MICROSOFT Azure Dedicated HSM

Azure Dedicated Ayrılmış HSM, Azure'da şifreleme anahtarı depolaması sağlar. Özel HSM, en katı güvenlik gereksinimlerini karşılarken, FIPS 140-2 Seviye 3 onaylı cihazlara ve HSM cihazının tam ve özel kontrolüne ihtiyaç duyan kullanıcılar için uygun bir çözümdür. [5]

Microsoft, bir THALES Group üyesi olan Gemalto'nun ürünü olan SafeNet Luna ağ HSM 7 (model A790) gerecini kullanarak Dedicated HSM hizmetini sunar.

MICROSOFT Azure Dedicated HSM özellikleri:

- FIPS 140-2 düzey 3 uyumluluğu: Azure Dedicated HSM, FIPS 140-2 düzey 3 gereksinimlerini karşılayarak finansal hizmetler sektörünün, devlet kurumlarının ve diğer kullanıcıların şifreleme anahtarı depolama konusundaki katı sektörel düzenlemelerini karşılar.
- Tek kiracılı cihazlar: Azure Dedicated HSM kullanıcılara dağıtık Microsoft veri merkezlerinde bulunan fiziksel bir

cihazı sağlayarak söz konusu cihaza sadece kullanıcının erişebilmesini sağlar.

- Özel Bulut Tabanlı Sistem: Microsoft FIPS 140-2 düzey 3 tarafından doğrulanan özel bir HSM hizmeti sunan ve bulut tabanlı ve şirket içi uygulama entegrasyonu sunan, tek bulut sağlayıcıdır.
- Yüksek Performans: Microsoft Azure Dedicated HSM, Gemalto tarafından yapılan, yüksek kapasiteli, performanslı ve düşük gecikme süreli cihaz sayesinde, geniş bir API desteği ve geniş kapsamlı bir şifreleme algoritması desteğini çok sayıda desteklenen işletim sistemi ile birlikte sunar. RSA 2048 için saniyede 10000 işlem performansı sunar.
- Tam Yönetim Denetimi: Cihaz dağıtıldıktan sonra kullanıcı dışında kimsenin cihaz üzerinde uygulama düzeyinde veya yönetici olarak erişimi yoktur.
- Azure Ayrılmış HSM kullanıcıları kuruluşlarındaki HSM'lere erişebilecek kişiler ve kişilerin rollerinin kapsamları ile birlikte atamalarını yönetirler. Kullanıcıya HSM'ler üzerinde tam yönetim ve şifreleme denetimi sağlanırken, Microsoft HSM'ler üzerinde depolanan anahtarları göremez veya bu anahtarlara erişemez [6].
- Yüksek Güvenlik: eIDAS Common Criteria EAL4+ ve FIPS 140-2 düzey 3 doğrulanmasına sahip olan Microsoft Azure Dedicated HSM dışarıdan müdahaleye dayanıklı olmakla beraber önemli sayıda uyumluluk ve güvenlik gereksinimini karşılar.

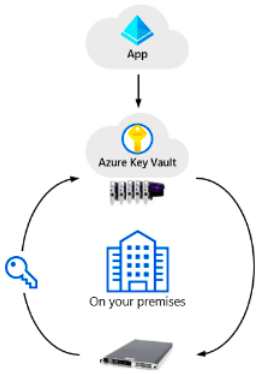

Fig. 2. Azure Key Vault HSM [14]

D. GOOGLE Cloud Key Management

- Şifreleme anahtarlarını merkezi bir şekilde yönetme: Kullanıcılar asimetrik veya simetrik fark etmeden anahtarlarını kurumların yönettiği gibi bulutta barındırılan anahtar yönetim sistemi üzerinden yönetebilir. AES256, RSA 2048, RSA 3072, RSA 4096, EC P256 ve EC P384 şifreleme anahtarlarını oluşturabilir, kullanabilir, döndürebilir veya kaldırabilir.[7]
- HSM aracılığı ile donanım anahtar güvenliği sağlanması: Donanım ve yazılım tabanlı şifreleme anahtarları arasında geçişin kolayca sağlanması. FIPS 140-2 Seviye 3 onaylı HSM'lerde şifreleme işlemlerinin gerçekleştirilmesi ve şifreleme anahtarlarının barındırılması.

Google Cloud HSM: Google Cloud Key Management servislerine dahil olan Google Cloud HSM bulut tabanlı bir donanım güvenlik modülüdür. Cloud HSM kullanıcıya, FIPS 140-2 düzey 3 doğrulanmış donanım güvenlik modülleri kümesi üzerinde kriptografik işlemler yapma imkanını kümeleme, ölçekleme veya yama yapma işlemlerini Google Cloud Key Management Servisleri yardımı ile gerçekleştirerek sunar. [8] Google Cloud HSM belirli müşterilerine tek kiracılı sistemler de sunmaktadır.

E. Alternatif Bulut Tabanlı Donanım Güvenlik Modülü Sistemleri

- IBM Cloud HSM [12]
- Alibaba Key Management Service [13]

IV. Bulut Tabanlı Donanım Güvenlik Modüllerine Yönelik Saldırılar

Yapılmış olan araştırmalar donanım güvenlik modüllerinin de hacklenebilir olduklarını gösteriyor. Kimliği doğrulanmamış saldırganlar, donanım güvenlik modüllerinin kontrolünü ele geçirerek içerisinde saklı olan veriye erişmişlerdir.

Bir donanım güvenlik modülünün saldırıya uğrayıp bilgilerinin ve saklamakta olduğu anahtarlarının ele geçirilmesinin kötü yanlarından biri ise güvenliği donanım modülüne bağlı olan çok hassas sistemler olsa bile, donanım güvenlik modüllerine kısa sürede yama yapma işleminin önemli ölçüde zor olmasıdır. [9]

Bulut donanım güvenlik modülleri ise, donanım güvenlik modülü olan bir donanıma bağlı olduğundan, bir soyutlama düzeyinde, aynı tür saldırılara karşı savunmasız halde oldukları söylenebilir.

V. POC Uygulama

POC uygulama geliştirme amacıyla Google Cloud HSM kullanılmıştır. Kullanıcılarına bulut tabanlı donanım güvenlik modülü hizmeti vermektedir. Bu HSM cihazlarını dünyanın dört bir yanında bulundurmaktadır. Müşteri, cihazın konumunu kendi belirlemektedir. Sundukları API ile kullanıcı aldığı hizmeti kolaylıkla kullanabilmektedir.

API kullanabilmek için öncelikle Google Cloud Projesi oluşturulmalı, ardından faturalandırma ve API konsoldan açılmalıdır. Uygulaması yapılan metodlar şu şekildedir.

- Anahtarlık Oluşturma: Bir HSM anahtarı oluşturulduğunda, seçilen bir Google Cloud konumundaki anahtarlığa eklenir. HSM modülünü destekleyen bir konumda yeni bir anahtarlık oluşturabilir veya mevcut olanı kullanılabilir. Anahtarlık oluştururken bir proje ve lokasyon belirtilir.
- HSM Anahtarı Oluşturma: Anahtarlığınız oluştuktan sonra, proje, lokasyon ve anahtarlık bilgisini vererek bir HSM anahtarı oluşturulur.
- Veri Şifreleme: HSM anahtarı oluşturduktan sonra bir metin veya binary dosya bu anahtar ile şifrelenir.
- Şifre Çözme: Şifrelenen metin veya binary dosya anahtar ile tekrar çözülür.

Fig. 3. Google Cloud HSM Lokasyonları

Sonuç olarak, Google Cloud HSM ile bu sistemlerin kolaylıkla kullanılabildiği anlaşılmıştır. Kayıt süreci ve kredi kartı bilgilerini verdikten sonra, çok kısa bir sürede anahtar oluşturup kullanılabilmektedir. Dokümantasyon ve API kullanımı oldukça kolaydır. Aynı zamanda kullanıldığı kadar ücret ödenmektedir. Bu sebeple kurulum maliyeti düşüktür.

VI. HSM ve HSM Cloud Farkları

- Fizikler HSM kurulum maliyetleri oldukça yüksek, bulut tabanlılarda ise düşüktür.
- Fizikler HSM'ler fiziki olarak belli şartlar gerektirmektedir, bulut tabanlılarda ise bu sorun yoktur. Mesela güvenlik sistemi gerekmektedir.
- Türkiye'de fiziksel HSM cihazları Kamu Sertifikasyon merkezi tarafından tastiklenebilir, fakat bulut tabanlı sistemler için henüz bir yasal düzenleme yoktur.

VII. Türkiye ve Bulut Tabanlı Donanım Güvenlik Modülleri

Kamu Sertifikasyon Merkezi donanım güvenlik modülü sertifikalandırma işlemini "Müşterinin kendisinin temin ettiği HSM cihazı kullanılmak isteniyorsa, sertifika yerinde gözetim ve denetim ile cihaza yüklenir" şeklinde belirtmiştir. Buna göre, Türkiye'deki bir HSM cihazı sertifikalandırılacak ise gözetim ve denetim altında bu işlem gerçekleştirilmelidir. Firmaların sunduğu bulut tabanlı HSM sistemleri ise farklı lokasyonlarda bulunmaktadır. Araştırmalara göre Türkiye'de bu hizmeti sunan bir firma yoktur. Google Cloud HSM Lokasyonları figüründe görüldüğü üzerinde dünyanın çok farklı konumlarında bulunmaktadır. Dolayısıyla, bir kullanıcı veya firma Türkiye'de bulut tabanlı donanım güvenlik modülü kullanabilir. Fakat Kamu Sertifikasyon Merkezi ile sertifikalandırma yapamaz.

Bunun yapılabilmesi için birkaç farklı yöntem geliştirilebilir. İlk çözüm olarak, bulut tabanlı donanım güvenlik modülü hizmetini veren firmanın Türkiye'de olması ve HSM cihazlarını Türkiye'de bulundurması olabilir. Bu sayede Kamu Sertifikasyon Merkezi yerinde inceleyebilir ve sertifika verebilir. Anlaşmalı bir şekilde firma buradan HSM hizmeti alabilir. İkinci bir yöntem ise, yurtdışında bulunan bir bulut tabanlı donanım güvenlik modülü firmasının Türkiye'de açacağı bir ofis ile ve yapılan Kamu Sertifikasyon Merkezi anlaşması ile kullanıcıya hizmet sağlaması olabilir. Kullanıcı bu firmadan aldığı hizmeti, Kamu Sertifikasyon Merkezi'ne tastikletebilir.

İlk çözüm yönteminde, Kamu Sertifikasyon Merkezi donanım güvenlik modülleri kümesine doğrudan Türkiye Cumhuriyeti sınırları içerisinde erişim sağlayıp onaylayabilir. Bu sayede herhangi bir yasal düzenleme olmadan kullanıcılar, Kamu Sertifikasyon Merkezi tarafından tasdiklenmiş donanım güvenlik modüllerini bulut tabanlı bir şekilde kullanabilir.

Fakat ikinci yöntem için çeşitli yasal düzenlemeler gereklidir. Çünkü Kamu Sertifikasyon Merkezi tasdik işlemini yerinde denetim yapmadan yapmak durumunda kalacaktır. Bunun yerine firma denetimi yapıp onun verdiği hizmete güvenmesi gerekmektedir.

VIII. Sonuç

Donanım güvenlik modülleri kimlik doğrulama için kullanılan sayısal anahtarların yönetimini ve korunmasına sağlayan fiziksel bir aygıttır. Common Criteria, FIPS 140 ve EIDAS gibi standartlara uygun bir şekilde sertifikalandırılmaktadırlar. Bulut tabanlı donanım güvenlik modülleri ise donanım güvenlik modülü hizmetini bulut aracılığı ile uzaktan sunan sistemlerdir. Amazon, THALES, Google ve Microsoft başta olmak üzere çeşitli şirketler bu hizmeti kendilerine has mimarileri ve özellikleri ile sunmaktadırlar. Yapılmış olan POC uygulama geliştirme ile, hem düşük maliyet hem de kısa bir süre içerisinde, Google tarafından sunulmuş olan uygulama programlama arayüzü sayesinde kullanıcıların bulut tabanlı donanım güvenlik modülüne kolaylıkla erişip kullanabileceği ispatlanmıştır. Fiziksel aygıt olan donanım güvenlik modülleri ve bulut tabanlı donanım güvenlik modülleri arasındaki farklar belirtilmiştir. Önemli sayıda avantajının yanı sıra donanım güvenlik modülleri her türlü saldırıya karşı dayanıklı olmamakla beraber saldırıya uğrayıp ele geçirilmiş donanım güvenlik modülleri için saldırıya karşı cevap vermek önemli ölçüde zordur, dolayısıyla bulut tabanlı donanım güvenlik modülleri de donanım güvenlik modüllerini kullandıkları için saldırılara karşı tam anlamıyla güvenli değildir. Türkiye Cumhuriyeti'nde donanım güvenlik modülleri TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi tarafından sertifike edilmektedirler. Bulut tabanlı güvenlik modüllerinin de sertifikasyon işlemine tabi tutulmaları için bu hizmeti sunan şirketlerin Türkiye Cumhuriyeti sınırları içerisinde donanım güvenlik modülü merkezi açmaları ve oradaki donanım güvenlik modüllerini sertifike ettirmeleri olası bir çözümdür.

References

[1] Hardware security module. (2020, October 31). Retrieved December 02, 2020, from Wikipedia
[2] Cloud HSM — Cloud KMS Documentation — Google Cloud. (n.d.). Retrieved December 02, 2020, from Google Cloud KMS
[3] Retrieved December 06, 2020, from Amazon AWS
[4] Retrieved December 06, 2020, from Thalesgroup
[5] Retrieved December 06, 2020, from Microsoft
[6] Retrieved December 06, 2020, from Microsoft Azure
[7] Retrieved December 06, 2020, from Google Cloud KMS
[8] Retrieved December 06, 2020, from Google Cloud HSM

[9] How to Hack a Hardware Security Module (HSM). (2020, September 29). Retrieved December 12, 2020, from Unboundtech Blog
[10] Mali Mühür Sertifika Hizmetleri Süreçleri. (n.d.). Retrieved December 12, 2020, from Kamu SM
[11] Retrieved December 12, 2020, from Cloud IBM
[12] Retrieved December 12, 2020, from Alibaba Cloud
[13] Retrieved December 12, 2020, from THALES Safenet Luna HSM 7
[14] Retrieved December 12, 2020, from Microfost Docs