Fırat Üniversitesi Müh. Bil. Dergisi
33(1), 113-123, 2021

Sis Bilişim: Güvenlik Boyutları ve Güvenlik Analizi

Fatih TOPALOĞLU[1*]
Bilgisayar Mühendisliği Böl., Mühendislik ve Doğa Bilimleri Fak., Malatya Turgut Özal Üniversitesi, Malatya, Türkiye
[*1] fatih.topaloglu@ozal.edu.tr

(Geliş/Received: 18/06/2020; Kabul/Accepted: 01/01/2021)

Öz: Sis bilişim, bulut bilişimi ağların kenarına kadar genişleten bir paradigmadır. Sis bilişimin öne çıkan özelliği dağınık ve son kullanıcılara yakın hizmetler sunmasıdır. Bu özellik, gizliliğin ve verilerin güvenliğinin korunması açısından çok önemlidir. Çünkü, sis bilişimin dağıtılmış mimarisi saldırı vektörlerinin sayısını arttırarak uç cihazların sahip olduğu verileri daha savunmasız hale getirir ve kötü amaçlı yazılım sızmalarına ve güvenlik açıklarına neden olur. Makale sis bilişim ortamındaki çeşitli güvenlik unsurlarının boyutlarını ve kapsamlı teknik analizini içermektedir. Bu çalışma iki nedenden dolayı ele alınmıştır. Birincisi, güvenlik, IoT sistemleri arasında belki de en büyük teknik kaygıdır, dolayısıyla özel bir çalışma olarak ele alınması gerekmektedir. İkincisi, çalışma son derece teknik ayrıntılar içerdiğinden güvenlik uzmanlarının en çok ilgi duyduğu bilgilerin bir kaynakta toplanması amaçlanmıştır.

Anahtar kelimeler: Sis bilişim, güvenlik boyutları, güvenlik analizi.

Fog Computing: Security Dimensions and Security Analysis

Abstract: Fog computing is a paradigm that extends cloud computing to the edge of the networks. The prominent feature of fog computing is that it provides services that are messy and close to end users. This feature is very important to protect privacy and data security. Because, the distributed architecture of fog computing increases the number of attack vectors, making the data that end devices have more vulnerable and cause malware infiltration and vulnerabilities. The article includes the dimensions and comprehensive technical analysis of various security elements in the fog computing environment. This study is discussed for two reasons. First, security is perhaps the biggest technical concern among IoT systems, so it needs to be addressed as a special study. Secondly, since the study contains highly technical details, it is aimed to gather information that security experts are most interested in a source.

Key words: Fog computing, security dimensions, security analysis.

1. Giriş

Sis bilişim, milyarlarca bağlı cihaz için yeni uygulamalar ve hizmetler sunabilen, doğrudan ağın kenarında işlem gerçekleştirebilen bilgi işlem platformudur. [1]. Sis bilişimin karakteristik özellikleri ,bant genişliğinden tasarruf, hareketlilik desteği, düşük gecikme ve gerçek zamanlı etkileşimler, heterojen, coğrafi dağılım ve merkezi olmayan veri analitiği, veri güvenliği ve gizlilik koruması, düşük enerji tüketimi ve birlikte çalışabilirliktir.

Sis bilişim, IoT uygulama dağıtım platformları [2-9], sağlık hizmetleri [10-13], akıllı şehir uygulamaları [14-17], hızlı tepki ve düşük enerji harcama [18,19] alanlarında gelişmiş hizmet kalitesi sunabilir. Ayrıca, sis bilişimde işbirliğinin gerçekleştiği birçok alan vardır. Bu gizlilik ve güvenlikle ilgili sorunlara yol açabilir. Sorunlu alanlar kimlik doğrulama ve yetkilendirme, kimlik yönetimi, kaynak erişim kontrolü, güvenli bir şekilde dağıtılmış karar yürütme ve işbirliği, güvenlik ve hizmet kalitesi, bilgi paylaşım politikası alanlarıdır [20-21].

Makale sis bilişim için kritik ve sorunlu bir alan olan güvenlik konusunu işlemektedir. Birlikte çalışabilirlik ve korumayı sağlamak için ortak bir güvenlik temelinin olması gerekmektedir. Ancak IoT platformu da dahil olmak üzere sis bilişim teknolojilerinde gereken tüm güvenlik mekanizmalarını belirlemek için henüz tamamen bütünsel bir güvenlik çözümü geliştirilmemiştir.

Ayrıca, sis hesaplama yerine getirmesi gereken bölgesel ve devlet gerekliliklerinin bir kombinasyonudur. Güvenlik analizi için belirlenen yöntemlerin en önemli avantajı sis mimarisinin güvenlik alanında birleşik bir uygulama oluşturması ve çeşitliliği barındırmasıdır. Çalışmada ileri sürülen sis bilişim güvenlik platformu, verimlilik yönetimi, güvenlik noktası, güvenilir yürütme modu gibi bir çok donanım güvenlik işlemcisi uygulamalarını da içermektedir.

[*] Sorumlu yazar: fatih.topaloglu@ozal.edu.tr. Yazarın ORCID Numarası: [1] 0000-0002-2089-5214

Çalışmada belirlenen güvenlik yöntemlerinin bir diğer avantajı uç aygıtlar ve bulut bilgi işlem veri merkezleri arasında dağıtılan yaygın bir bilgi işlem altyapısı sunularak, yalnızca yüksek kullanılabilir gerçek zamanlı güvenilir bilgi işlem hizmetleri sunma yeteneğine sahip olmakla kalmaması, aynı zamanda dinamik çok katmanlı savunma uygulamaları için de iyi bir konuma sahip olmasıdır.

Sis bilişim verileri buluta taşıyan birçok basamaktan oluşur. Bu katmanlar karmaşıklıkları ve veri dönüşümlerini kapsar. Çalışmada mimari detaylarda yer alan performans, yönetilebilirlik, veri analizi ve benzer ayrıntı seviyelerine sahip kontrol gibi yüksek öncelikli perspektifleri tanımlayan bilgiler içermekle birlikte sis bilişimin güvenlik boyutları belirlenerek daha derin güvenlik analizi yapılmıştır.

Makalenin akışı, ikinci bölümde sis mimarisinin şifreleme işlemleri boyutu, üçüncü bölümde sis düğümlerinin güvenlik boyutu, dördüncü bölümde sis mimarisinin ağ güvenliği boyutu ve beşinci bölümde veri güvenliği boyutları için teknik güvenlik analizleri yapılmıştır.

2. Şifreleme İşlemleri Boyutu

Son kullanıcılara yakın olarak sis düğümleri, haksız saldırılara karşı savunmasız hale gelebilir [22-23]. Ancak bu sorun, şifre çözme ve şifreleme yaklaşımlarıyla etkin bir şekilde çözülebilir. Ayrıca, sis düğümleri genellikle bulut bilişimdeki uç cihazlarla ve veri havuzlarıyla etkileşime girmelidir.Tüm bu karmaşık işlemler, verileri saldırıya açık ve savunmasız hale getirir. Bu sorunu çözmek için maskeleme teknikleri veya şifreleme algoritmaları kullanılmaktır [24].

Sis mimarisinde şifreleme işlemleri gizlilik, bütünlük, kimlik doğrulama ve reddedilmeme gibi güvenlik hizmetlerini uygulamak için mekanizmalar sağlar. Şifreleme işlemleri, diğer nesneleri koruyan şifreleme anahtarlarını ve güvenlik ilkelerini korumak için bir güvenlik işlemcisinde uygulanmaktadır. Ayrıca, güvenilir yazılım için güvenli bir yürütme ortamı sağlamak, bellek, depolama ve reddedilmeme işlemlerini korumak için de kullanılmaktadır.

Sis hesaplama uygulamalarında; gizliliğin korunması için simetrik veya gizli anahtar şifreleri, kimlik doğrulama için şifreleme karma işlemleri, gizli anahtar, güvenlik kimlik bilgileri ve reddedilmeme için asimetrik veya ortak anahtar şifreleri kullanılabilir.

2.1. Kriptografik hızlandırıcı

Kriptografik hızlandırıcı , yoğun kriptografik işlemleri CPU' da çok daha verimli bir şekilde gerçekleştirmek için özel olarak tasarlanmış bir ortak işlemcidir. Birçok sunucunun sistem yükü çoğunlukla şifreleme işlemlerinden oluştuğu için, bu işlemci ile sunucu performansını büyük ölçüde arttırmaktadır. Kriptografik işlemlerin ve şifreleme hizmetlerinin önemli bir yavaşlama belirtisi göstermemesi, kriptografiyi hem iş hem de kişisel veri korumada siber güvenlik sisteminin önemli bir parçası haline getirdi. Sis hesaplama uygulamalarında kriptografik hızlandırma yalnızca yazılım algoritmalarıyla değil, sağlanacak ek donanımlar ile de gerçekleştirlmektedir.

Sis bilişimde bu sistemlerin nasıl entegre edileceğine bağlı olarak bilgisayar donanımına kriptografik hızlandırma getirmenin bir kaç faydası vardır. Bunlardan en önemlisi donanımlarının diğer operasyonel yönlere odaklanmasını sağlaması ve böylece donanım performansı ve operasyonel yetenekte önemli bir artış getirmesidir. Diğer avantajı gelişmiş güvenlik, sadece bu tür bir ortamda çalışmak üzere özel olarak tasarlanmış değil, aynı zamanda imalatçıların yetenekleri ile ilgili iddialarını test etmek için üçüncü taraflarca titizlikle test edilmiş olan donanım veya yazılımı kullanarak, hesaplama kaynakları sağlamak için güvenlik unsurlarından yararlanabilir.

Böylelikle kriptografik hızlandırma, ağ cihazlarında ve sunucularında giderek yaygınlaşan bir özellik haline gelebilir. Şifreleme ve şifre çözme, yeterli düzeyde koruma ve güvenlik gerektiren işletmeler ve bireylerin CPU'ları üzerindeki yükü azaltmalarını sağlayan araçlar korumayı sağlamak için muhtemelen bu gibi sorunlara çözüm önerisi olarak sunulabilir.

2.2. Gerçek rastgele sayı üreteci

Birçok alanda rastgele sayılar gereklidir: kriptografi, Monte Carlo hesaplama ve simülasyonu, endüstriyel test ve etiketleme, tehlike oyunları, kumar vb. Bilgisayarlar deterministik olarak çalıştıklarından rastgele sayılar üretemezler. Bunun yerine rastgele sayılar iyi kontrol edilen ve özel olarak hazırlanmış bir fiziksel prosesi ölçerek çalışan gerçek rastgele sayı üreteçleri (TRNG) kullanılarak elde edilir. Bir TRNG'nin rastgele olması kesin, bilimsel olarak karakterize edilebilir ve ölçülebilir.

Sis hesaplamada TRNG, bir algoritma yerine fiziksel bir işlemden rastgele sayılar üreten bir cihazdır. Bu tür cihazlar genellikle termal gürültü, bir ışın ayırıcıyı içeren fotoelektrik etki ve diğer kuantum fenomenleri gibi düşük seviyeli, istatistiksel olarak rastgele "gürültü" sinyalleri üreten mikroskobik fenomenlere dayanır. Bu, bilgisayar programlarında yaygın olarak uygulanan sözde rastgele sayı üretme paradigmasının tersidir .

Gerçek rastgele sayı üreteçleri tipik olarak, fiziksel olayların bazı yönlerini bir elektrik sinyaline dönüştüren bir dönüştürücüden , rastgele dalgalanmaların genliğini ölçülebilir bir seviyeye yükseltmek için bir amplifikatör ve diğer elektronik devrelerden ve bir tür analogdan çıkışı dijital bir sayıya dönüştürmek için dijital dönüştürücü, genellikle basit bir ikili basamak 0 veya 1'dir. Rastgele değişen sinyali tekrar tekrar örnekleyerek bir dizi rastgele sayı elde edilir.

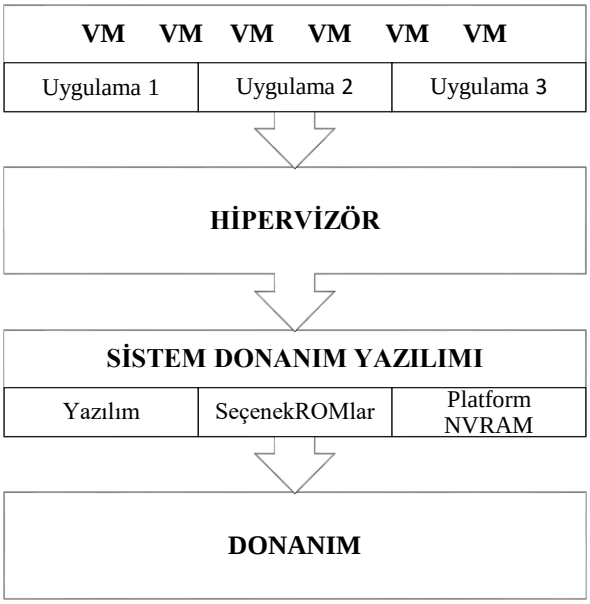
Sis bilişim platformunda TRNG, ana uygulama içinde rastgele kriptografi oluşturmak, güvenli veri iletimi için şifreleme anahtarları ve aktarım katmanı güvenliği gibi internet şifreleme protokollerinde yaygın olarak kullanılabilir.

2.3. Güvenli anahtar üretimi, şifreleme ve depolama

Kriptolojide anahtar üretimi zorlu bir görevdir çünkü Kerckhoff prensibine göre saldırganın şifreleme sistemi hakkında anahtar haricinde her şeye ulaşabildiği varsayımı altında sistemin ne kadar güvenli olduğu değerlendirilmektedir [25].Tüm işlemciler platform güvenlik işlemcisi olarak bilinen küçük bir yonga içerir. Bu teknoloji sis bilişimde bellek şifrelemesinden ve platform güvenliğinden sorumlu bir güvenlik yongası olmakla birlikte uzaktan yönetim için de kullanılabilir. Sertifikalar, anahtarlar ve şifreler için güvenli bir kasa görevi görebilir ve pahalı jetonlara olan ihtiyacı ortadan kaldırabilir.

3. Düğüm Güvenliği Boyutu

Bilgisayarların veri merkezleri altyapısı için en çok “hipervizör tabanlı sanallaştırma teknolojileri” ve bulut bilişim diye bilinen “konteyner teknolojileri” kullanılmaktadır. Bu iki teknoloji; verimlilik, yönetim kolaylığı, güvenlik gibi birçok faydaları nedeniyle tercih sebebidir. Yapılan çalışmada hipervizör tabanlı sanallaştırma mimarisi kullanıldığı varsayılarak analiz yapılmıştır. Sis bilişim çözümlerinde sanallaştırma şart olmadığı gibi, kullanılmaması halinde hipervizör katmanına da ihtiyaç ortadan kalkacaktır.



Şekil 1. Düğüm güvenliği mimarisi.

Düğüm mimarisi Şekil 1'de dört yatay bölgeye ayrılmıştır: Birincisi, en altta harici cihazlar dahil donanım bileşeni katmanıdır. Burada bir dizi isteğe veya kullanım durumuna bağlı donanım hızlandırıcıları, şifreleme cihazı ve jenerik hızlandırıcılar bulunmaktadır.

İkincisi sistem donanım yazılımı, seçenek ROM'ları ve Platform NVRAM bulunur. Bu bileşenlerin doğası ve varlığı platforma bağlıdır. Kök güvenilirlik ve güven zinciri uzantısını desteklemek için, açıldıktan sonra platformda çalıştırılacak ilk kod olan güvenilir sistem ROM'unda yerleşik bir üretici yazılımı uygulaması olmalıdır.

Üstünde Hipervizör katmanı vardır. Sanal aygıt örneklerini başlatır, yönetir, bunları işlemler, yönetim ve idare sistemi tarafından yönlendirildiği gibi sanal makinelere atar. Bu sanal cihazlar, veri için hipervizörü atlayan veya yazılım tarafından taklit edilen sanal örnekler olarak tamamen desteklenebilir.

Son katman, sanal makinelerin başlatıldığı katmandır. Fiziksel kaynaklar burada hipervizör tarafından sanal kaynaklar olarak eşleştirilir. Sanal makinelerdeki işletim sistemi, ayrı uygulama adres alanları veya Linux kapsayıcıları olarak başlatılabilecek uygulama adres alanlarını yönetir.

Sis mimarisinde katmanları bağlayan ve güvenilir bileşenlerden oluşan güvenli bir Güven Zinciri oluşturmaya yardımcı olan sistem hizmetleri sağlayan bir dizi işlev vardır. Sis mimarisinde, güvenilir yürütme ortamını başlatan ve hipervizöre hizmet veren güvenlik motorudur. Yönetici hipervizör katmanında gösterilen sanal güvenlik motorunu, her güvenilir sanal makinede yerleşik bir araçla sanallaştırır.

Bir diğer işlev, sanal makineyi içeren bir güven zinciri oluşturmak için her bir firma yazılımı veya yazılım yükünü doğrulayan ve ölçen güvenilir önyükleme yazılımıdır. Sis platformunda güvenilir önyükleme mekanizması yazılımı birbirini izleyen her kod yükünün güven zincirinin genişletilmesine izin vermek ve güvenilir olmasını sağlamak içindir.

3.1. Çalışma zamanı bütünlük denetimi

Sis mimarisinde bir saldırganın sistem çalışırken yazılımı değiştirmeye çalışması da muhtemeldir. Bu amaçla doğrudan XIP NOR flaşında veya NAND flaş uygulamaları için harici RAM'de yazılım görüntüsünü önyükleme sonrası periyodik olarak doğrulayan çalışma zamanı bütünlük denetimi özelliğine ihtiyaç vardır. Çalışma zamanı bütünlük denetimi işlemi, çalışma zamanı değişikliklerini karşılamak için küçük değişiklikler yaparak güvenli önyükleme işlemine benzer.

Çalışma zamanı bütünlük denetimi işlevi, kendi atanmış RAM'i olan bir güvenli yürütme ortamında çalıştırılmalıdır; burada çalışma zamanı bütünlük denetimi işlevine bir saldırgan tarafından müdahale edilmediği garanti edilir. Bir saldırganın çalışma zamanı bütünlük denetim kodunu veya çalışma zamanı bütünlük denetimini ilk olarak çağıran prosedürü değiştirmeye çalışabileceği düşünüldüğünde, çalışma zamanı bütünlük denetiminin bir güvenli yürütme ortamında çalışması gerektiği açıktır. Güvenli yürütme ortamı ayrıca, periyodik olarak çalışma zamanı bütünlük denetimi işlevini tetikleyen bir güvenli zamanlayıcıya sahip olmalıdır.

Sis uygulamalarında yazılım bütünlüğünün korunmasına yardımcı olan isteğe bağlı mekanizmalar, birden fazla anahtar çiftinin desteklenmesi gerektiği durumlarda anahtar yönetimi için bir yazılım mekanizmasını içerir. Yazılım sürümü iptal mekanizması, üreticinin sistemi yeni bir yazılım sürümüne ilerletmek ve eski bir sürüme geri dönmeyi önlemek isteyebileceği uzun ömürlü sistemler için önemlidir.

Böyle bir durumda, güvenli önyükleme imzasının bir parçası olarak bir yazılım sürümü sayacı bağlanır ve bu mekanizma etkinleştirilir. Sis bilişimde çalışma zamanı bütünlük denetimi yazılım görüntüsünün bütünlüğünü sürekli olarak kontrol ederek çevrimiçi saldırıları gerçek zamanlı olarak belirleyebilir.

3.2. Hata ayıklama, performans izleme ve profil kontrolü

Tersine mühendislik koruması, aygıt çalışırken ve çip belleğinde kod bulunduğunda güvenlik operasyon merkezine (SoC) fiziksel erişimi önleyerek yetkisiz hata ayıklamayı JTAG aracılığıyla önleyen bir Güvenli Hata Ayıklama özelliği de gerektirir.

Cihazın kopyalanmasını önlemek için flaş bellekte bulunan yazılım görüntüsü benzersiz bir anahtar kullanılarak şifrelenir. Yalnızca belirli bir SoC, yazılım görüntüsünün şifresini çözerek yazılımı belirli bir yongaya etkili bir şekilde bağlayabilir. Sis mimaride klonlanan herhangi bir cihaz, yazılım görüntüsünün şifresini çözemez ve bu da cihazı işe yaramaz hale getirir.

4. Ağ Güvenliği Boyutu

Uç aygıtlar ve bulut bilgi işlem veri merkezleri arasında dağıtılan güvenli bir sis platformu, yalnızca yüksek kullanılabilirlik ve gerçek zamanlı bilgi işlem hizmetleri sunma yeteneğine sahip olmakla kalmayıp aynı zamanda dinamik çok katmanlı savunma için de iyi bir konuma sahiptir.

Şekil 2. Operasyonel düzlemler ve işlevsel katmanlar.

Şekil 2'de Güvenlik Sağlama ve Güvenlik İzleme iki operasyonel düzlemleriyle uçtan uca güvenlik sağlayan mimariyi göstermektedir. Güvenlik Sağlama Yönetimi, İletişim Güvenliği, Hizmet Güvenliği ve Uygulama Güvenliği olmak üzere üç işlevsel katmandan oluşur.

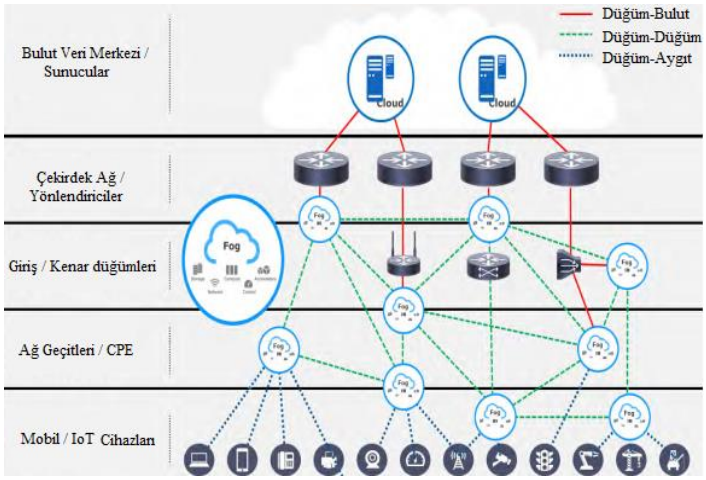
4.1. İletişim güvenliği katmanı

Aygıttan buluta iletişim genellikle TCP veya UDP kanalları üzerinden gerçekleşir. TCP bağlantı yönelimli ve güvenilirdir, yani gönderilen her veri paketinin alındığını onaylaması gerekir. Ancak büyük güvenilirlik ile büyük yük gelir ve bazen bir IoT uygulaması için TCP başlığı, yükün kendisinden daha büyük olabilir. Öte yandan UDP, bağlantısız ve güvenilmezdir, yani hız açısından veri paketlerinin kaybına izin verir. TCP, verilerin geçmesi gereken yerlerde kullanılırken, bazı veri kayıplarının kabul edilebilir olduğu yerlerde UDP kullanılır. Bu katman, Cihaz-Sis-Bulut Bilişim Hiyerarşisindeki tüm varlıklar arasındaki tüm fiziksel veya sanal iletişim kanallarında Tablo 1'deki iletişim güvenliği hizmetlerini uygular.

Tablo 1. İletişim güvenliği.

Gizlilik	Bütünlük	Kimlik Doğrulama	Reddetmeme
Bağlantı ve Bağlantısız Veri Gizliliği	Kurtarma ile Bağlantı Bütünlüğü	Bağlantısız İletişim için Veri Kaynağı Kimlik Doğrulaması	Kaynağı Reddetmeme
Trafik Akışı Gizliliği	Algılama ile Bağlantısız Bütünlük	Bağlantı Tabanlı İletişim için Eş Varlık Kimlik Doğrulaması	Hedefin Reddedilmemesi
	Tekrar oynatma koruması	Kimliği Doğrulanmış Kanal Erişim Kontrolü	

Şekil 3'de gösterildiği gibi Cihaz- Sis- Bulut Bilişim sürekliliğinde gerçekleşen iletişim, Düğümden→ Buluta, Düğümden → Düğüme ve Düğümden→Aygıta gibi üç tür güvenli iletişim yolu olarak kategorize edilebilir.



Şekil 3. Güvenli iletişim yolları.

Düğümden Buluta Güvenli İletişim Yollarında, güçlü kimlik doğrulama ve reddetme hizmetleri, sis düğümüne kurulan donanım güven kaynağından türetilen güvenlik bilgileri kullanılarak uygulanacaktır. Tüm şifreleme işlemleri sis düğümlerine gömülü kripto hızlandırıcıları tarafından gerçekleştirilirken, şifreleme anahtarları güvenlik izleme ve yönetim işleminin bir parçası olarak yönetilecektir.

Düğümden Düğüme Güvenli İletişim Yollarında, dağıtılmış bir sis bilgi işlem platformu, birden fazla internet alt ağına veya yönetim alanına yayılmış sis düğümleri hiyerarşisinden oluşabilir ve bu sis düğümlerinin belirli hedefleri gerçekleştirmek için birbirleriyle koordinasyon yapmaları beklenir. Sis bilişimde hem doğrudan hem de zamanında etkileşimi sağlamak için, işleme dayalı istemci-sunucu bilgi işlem modeline ve olaya dayalı yayınlama-abone olma mesajlaşma modellerine dayalı düğümler arası bilgi alışverişleri uygulanacaktır.

Düğümden Cihaza Güvenli İletişim Yollarında, genellikle bulut sunucularının proxy'leri olarak işlev gören sis düğümleri iletişiminin, ön uç aygıtları tarafından kullanılan iletişim protokollerini ve API'leri koruması beklenir. Cihaz iletişim protokollerinin seçenekleri farklı uygulamalar ve iletişim ortamları arasında çeşitlendirilmiştir.

Sis Mimarisinde internet protokollerine uyarlanan ön uç aygıtları arasında, ön uç aygıtlarına verilen güvenlik kimlik bilgileri kullanılarak güçlü kimlik doğrulama uygulanabilir. Şifreleme anahtarları, güvenlik izleme ve yönetim işleminin bir parçası olarak yönetilebilirken, tüm şifreleme işlemleri ön uç aygıtlarındaki kripto özellikli yerleşik işlemciler tarafından gerçekleştirilebilir.

4.2. Hizmetler güvenlik katmanı

Yazılım tanımlı ağ uygulamalarının artan kullanımı ile özel cihazlar, sanal makinelerde ve Linux kapsayıcılarında yazılım çözümleri olarak giderek daha fazla uygulanmaktadır. Tablo 2'de listelenen cihazlarla birlikte, bu güvenlik cihazı kategorisine genellikle ağ fonksiyonu sanallaştırma veya bireysel olarak sanal ağ fonksiyonları denir. Bu katman, geleneksel olarak Tablo 2'deki hizmetleri sunar.

Tablo 2. Hizmetler güvenlik katmanı hizmetleri.

Ağ güvenliği aygıtları tarafından sağlanan bilgi güvenliği hizmetleri	**Güvenlik hizmetleriyle birlikte verilen ağ hizmetleri**
Derin Paket Denetimi (DPI)	vRouters
Uygulama Katmanı Proxy'si Ful Yasal Mesaj Durdurma	WAN Hızlandırıcıları
Saldırı Tespit ve Koruma Sistemleri (IPS / IDS)	Address Ağ Adresi Çevirmenler (NAT)
Sistem / Ağ Olayı ve Durum İzleme	İçerik Dağıtım Sunucuları
İçerik Filtreleme ve Ebeveyn Kontrolü	

Sis mimaride hizmet içi iletişim için kriptografik kimlik doğrulama ve yetkilendirme kullanılır. Bu, yöneticiler için soyutlama ve ayrıntı düzeyinde güçlü erişim kontrolü sağlar. Bununla birlikte IP sahtekarlığını önlemek için ağın çeşitli noktalarında giriş ve çıkış filtreleri kullanılmalıdır.

Bir hizmeti aynı makinede çalışan diğer hizmetlerden korumak için kullanılacak teknikler Linux kullanıcı ayrımı, dil ve çekirdek tabanlı sanal alanlar ve donanım sanallaştırmasıdır. Ayrıca riskli iş yükleri için daha fazla izolasyon katmanı kullanılmalıdır.

4.3. Uygulama güvenliği katmanı

Uygulama katmanı, kullanıcılar için bir kullanıcı arabirim görevi görür. Bu katmanın ana işlevi, farklı uygulamaların yönetimini kolaylaştırmaktır. Uygulama katmanı sis hiyerarşisinin ön ucudur ve bu nedenle perspektifli uygulamalar olarak farklı güvenlik standartlarına ihtiyaç duyar. Farklı uygulamaların farklı gereksinimleri olduğundan, bu seviyeyi güvenli hale getirme görevi çok karmaşık ve zordur. Güvenlik tehditleri, mevcut ve ağda kullanılan protokollere göre değişir. Sis platformu için ilgili protokoller MQTT, AMQP, CoPA ve XMPP'dir.

5. Veri Güvenliği Boyutu

Verilerin sis sisteminde bulunduğu üç genel kategori vardır: Kullanımdaki veriler, beklemedeki veriler ve hareket halindeki veriler.

5.1. Kullanımdaki veriler

Kullanılan veriler, bir sabit sürücüde veya harici depolama ortamında pasif olarak saklanmayan, bir veya daha fazla uygulama tarafından işlenen verilerdir. Ayrıca, çeşitli uç noktalardan erişen kullanıcılar tarafından görüntülenen verileri de içerir. Sis mimarisinde veriler, sistemde nerede olduğuna ve onu kimlerin kullanabildiğine bağlı olarak farklı tehdit türlerine karşı hassastır. Kullanımdaki veriler için en savunmasız nokta, kullanıcıların bu verilere erişebileceği ve onlarla etkileşime girebileceği uç noktalardadır.

Sis platformundaki bir veri kümesinin potansiyel olarak birden çok uç noktadan çalışan birden fazla kullanıcısı olabilir. Kişisel cihazlardan ana bilgisayar verilerine erişen çok sayıda şirket içi sistem, cihaz ve çalışan, bu verilerin güçlü kullanıcı kimlik doğrulaması, kimlik yönetimi ve profil izinleriyle korunması gerektiği anlamına gelir. Bu, yalnızca uygun izin ve bilgiye sahip kişilerin verilere erişmesini ve bunları değiştirmesini sağlar.

Bellek şifreleme, sis sistemini çeşitli saldırılara karşı korumak için ana bellek şifrelemesi kullanılabilir. Veriler günümüzde diskte bozulmadan şifrelenmiş olsa da, DRAM'da açık bir şekilde saklanır. Bu, verileri yetkisiz yöneticiler, yazılımlar ve donanım koruması ile gözetleme konusunda savunmasız bırakabilir. Şifreleme olmadan, hassas veriler, şifreler veya gizli anahtarlar kolayca tehlikeye atılabilir.

Sis mimaride tam bellek ve kısmi bellek olmak üzere iki farklı model ile bellek şifreleme yapılabilir. Tam bellek şifrelemeyle, tüm DRAM içerikleri, yapay önyükleme, DRAM arabirimi gözetleme ve benzer türden saldırılara karşı güçlü koruma sağlayan rastgele anahtar kullanılarak şifrelenir. Kısmı bellek şifrelemesi, yöneticiye ve işletim sistemine seçici olarak şifreleme esnekliği sağlar.

5.2. Beklemedeki veriler

Beklemedeki veriler, bir aygıtta veya yedekleme ortamında herhangi bir biçimde depolanan verilere karşılık gelen bir terimdir. Sabit sürücülerde, yedekleme bantlarında, tesis dışı bulut yedeklemesinde veya hatta mobil cihazlarda depolanan veriler olabilir. Veriyi bekletmeye iten şey, şu anda bir ağ üzerinden iletilmeyen veya aktif olarak okunmayan veya işlenmeyen etkin olmayan verilerdir.

Sis mimaride beklemedeki veriler bir hedefe ulaşmış verilerdir. Bu hedefe, şifreleme, çok faktörlü kimlik doğrulama ve hem dijital hem de fiziksel erişim kontrolleri gibi ek güvenlik katmanları eklenebilir. Beklemedeki veriler sis platformunun neresindeyse her zaman şifrelenmelidir.

Beklemede olan verilerin güvenliğini sağlamak ve şifrelemek için genellikle üç yöntem vardır:

Tam Disk Şifrelemesi, donanım düzeyinde şifrelemedir. Sis platformunda, bir cihazdaki tüm kullanıcı verilerini şifrelenmiş bir anahtar kullanarak kodlama işlemini gerçekleştirir. Bir aygıt şifrelendikten sonra, kullanıcı tarafından oluşturulan tüm veriler diske yüklenmeden önce otomatik olarak şifrelenir ve tüm okumalar, çağrı sürecine geri dönmeden önce verilerin şifresini otomatik olarak çözer.

Sis mimaride tam disk şifrelemenin avantajı, başlangıçta cihazın kilidini açtıktan sonra son kullanıcının özel bir dikkat gerektirmemesidir. Veri yazıldıkça, otomatik olarak şifrelenir. Okunduğunda otomatik olarak şifresi çözülür. Ancak işletim sistemi de dahil olmak üzere sabit sürücüdeki her şey şifrelendiğinden ,şifreleme ve şifre çözme işleminin, özellikle sanal belleğe yoğun bir şekilde erişimde veri erişim sürelerini yavaşlatabilir.

Dosya Sistemi Şifrelemesi, belirli dosyaları dosya, dizin ve klasör bazında korumak için ayrı bir anahtar tabanlı erişim ve kimlik doğrulama mekanizması kullanarak gerçekleştirir. Sis platformu simetrik şifreleme algoritması kullanır, çünkü büyük miktarda veriyi şifrelemek ve şifresini çözmek, asimetrik bir anahtar şifresinin kullanılmasından daha az zaman alır. Kullanılan simetrik şifreleme algoritması, işletim sisteminin sürümüne ve yapılandırmasına bağlı olarak değişecektir.

Dosya Sistemi Erişim Kontrol Mekanizmaları, kullanıcı kimliği veya grup kimliği ile belirli dosyalara veya dosya gruplarına erişimi kısıtlamak için kullanılabilir. Tüm modern dosya sistemleri dosya izinlerini bir biçimde uygular. Tablo 3'de gösterildiği gibi temel dosya izinleri, izin türleri kullanılarak izin gruplarına uygulanır.

Tablo 3. Dosya sistemi işlemleri için izin grupları ve türleri.

İzin Grupları	İzin Türleri
Kullanıcı izinleri: yalnızca dosyanın veya dizinin sahibi için geçerlidir.	Okuma izni: kullanıcının dosyanın içeriğini okuma yetkinliği. ifade eder.
Grup izinleri: yalnızca dosyaya veya dizine atanmış grup için geçerlidir.	Yazma izni: kullanıcının bir dosyayı veya dizini yazma veya değiştirme yetkinliği.
Tüm Kullanıcı izinleri: sistemdeki diğer tüm kullanıcılar için geçerlidir.	Yürütme izni: kullanıcının bir dosyayı yürütme veya bir dizinin içeriğini görüntüleme yetkinliği.

Erişim Kontrol Listesi sis mimarisinde bir dosya, klasör veya başka bir nesne için kullanıcı izinlerinin belirlendiği listedir. Kullanıcıların ve grupların hangi nesneye erişebileceklerini ve hangi işlemleri gerçekleştirebileceklerini tanımlar. Bu işlemler genellikle okuma, yazma ve yürütmeyi içerir.

5.3. Hareketli veri

Hareket halindeki veriler, bir sis platformunda şu anda bir ağ üzerinde seyahat eden veya okunmaya, güncellenmeye veya işlenmeye hazır bir bilgisayarın RAM'inde oturan verilerdir. Yerelden bulut depolamaya veya merkezi bir ana bilgisayardan uzak bir terminale ağlar üzerinden veri geçişi, verilerin kaynağı ve hedefi arasındaki herhangi bir makine veya bilgisayar korsanı tarafından okunamayacak veya değiştirilemeyecek şekilde şifrelenmelidir. Hareket halindeki bu veriler, kablolar arasında hareket eden verileri ve kablosuz iletimi içerir.

Şifreli bağlantı, gönderilecek bilgilerin şifreleme durumuna bakılmaksızın, ağ bağlantısı üzerinden gönderilen her şeyin otomatik olarak şifrelendiği bağlantıdır. Aktarım sırasında verileri harekete geçirmenin başka bir yöntemi de zaten şifrelenmiş bir dosya kullanmaktır. Şifrelenmiş bir dosya şifreli biçimde bulunduğundan, her zaman şifrelenir ve bu nedenle korunur.

6. Tartışma ve Öneriler

Şifreleme işlemleri boyutu gizlilik, bütünlük, kimlik doğrulama ve reddedilmeme gibi güvenlik hizmetlerini uygulamak için mekanizmalar sağlar. Daha önce yapılan çalışmalardan farklı olarak sis mimarisi, bileşenleri arasında birlikte çalışabilirlik seviyesini garanti etmek için yapılan çalışmada FIPS 140-2 [ref-a], [ref-b] şartnamesi referans alınarak çözüm önerileri sunulmuştur.

Mevcut uygulamalarda güvenlik işlemcisi genellikle işletim sistemi ile bire bir ilişki varsayar, böylece güvenlik işlemcisi işlevleri sanal bir ortamda yalnızca hipervizör tarafından kullanılabilir. Bu, sanal bir makinede yürütülen bir işletim sisteminin, çıplak metal bir ortamda çalışacağı için güvenlik işlemcisinin güvenli depolama ve şifreleme işlevlerini kullanabilmesine rağmen, bunu yapamayacağı anlamına gelir. Yapılan çalışmada çözüm önerisi olarak, sanal makinelerin çok sayıda tasarımı yerine mevcut kaynaklarla sınırlı, sanal platform güvenlik işlemcisi ile bire bir ilişki sürdürmesine izin veren bir sanal güvenlik işlemcisinin uygulanması sunulmuştur.

Donanım rastgele sayı üreteçlerinin ana kullanımı veri şifrelemedir, örneğin verileri şifrelemek için rastgele şifreleme anahtarları oluşturmaktadır. Bunlar, bilgisayarlarda yaygın olarak kullanılan rastgele sayılar üretmek için kullanılan Sahte Sayı Üreteçleri (PRNG) yazılımlarına daha güvenli bir alternatiftir. PRNG'ler sayısal diziler üretmek için hesaplanabilir bir algoritma kullanır.

Literatür çalışmalarında benimsenen PRNG'ler tarafından üretilen sayı dizisi tahmin edilebilir olduğundan, yalancı sayılarıyla şifrelenen veriler kripto analize karşı potansiyel olarak savunmasızdır. Donanım TRNG'leri tahmin edilemeyen sayı dizileri üretir ve bu nedenle verileri şifrelemek için kullanıldığında en yüksek güvenliği sağlar. Yapılan çalışmada, PRNG çözümünün aksine bir TRNG çözümü benimsenmiştir. Bu işlevsellik bir ISA uzantısı olarak veya ayrı bir hızlandırıcı cihaz aracılığıyla uygulanabilir.

Mevcut çalışmalarda düğüm güvenliğinde temel varsayım, hipervizörün kendisine güvenilmesi esasına dayanır. RTIC yalnızca sanal cihazları kontrol etmek için kullanılır. Sayfa mekanizmaları, yazılmaması gereken sayfalara yazmaları algılayacak şekilde değiştirildiğinden, kullanılan mekanizmalar çoğunlukla pasiftir. Yetkisiz bir değişiklik tespit etme eylemi politika tarafından yönlendirilir ve genellikle sanal cihazlarda sonlandırılır. Yapılan çalışmada bu sorun için şifrelenmiş bir "kapsayıcı" (Linux kapsayıcılar ile karıştırılmamalıdır) kod ve verileri dış saldırılardan koruyacak bellek şifrelemesi önerilmiştir.

Ağ güvenliği boyutu uygulamalarında yapılan çalışmada Güvenlik Sağlama, Güvenlik İzleme ve Yönetimi ve üç işlevsel katmanı: İletişim Güvenliği, Hizmet Güvenliği ve Uygulamaları Güvenliği diğer çalışmalardan farklı olarak ITU-X.805 Tavsiyesi [X.805] ve Açık Ağ Kurulumu tarafından önerilen Yazılım Tanımlı Ağ (SDN) Mimarisi [ONF / SDN] ile de uyumludur. Çalışmada iletişim güvenliği noktasında belirlenen paradigmaları uygulamak için belirlenen güvenlik protokolleri Tablo 4, 5 ve 6' da verilmiştir.

Tablo 4. Düğümden buluta iletişim için güvenlik protokolleri.

Uygulamalar	İşlem Protokolleri	Güvenlik Protokolleri
Kurumsal Uygulamalar	HTTP üzerinden SOAP Servis Odaklı Mimari	WSS
Mobil/Kişisel Uygulamalar	RESTful HTTP/ COAP Kısıtlı Uygulama Protokolü	TLS / DTLS

Tablo 5. Düğümden düğüme iletişim için güvenlik protokolleri.

Paradigmalar	İşlem Protokolleri	Güvenlik Protokolleri
Müşteri Sunucusu	SOAP, RESTful HTTP/ COAP	WSS, TLS/DTLS
Yayınla- Abone	MQTT, AMQP, RPTS	TLS/DTLS

Tablo 6. Düğümden cihaza iletişim için güvenlik protokolleri.

Katmanlar	Protokoller
MAC katmanı	WLAN, WPAN, PLC:PRİME
Taşıma Katmanı	UDP, TCP
Uygulama Katmanı	COAP, MQTT, AMQP, RTPS
Güvenlik	Güvenli Cihaz Kimliği Medya Erişim Kontrolü (MAC) Güvenliği Port Tabanlı (Kimlik Doğrulamalı) Medya Erişim Kontrolü Tünel / Taşıma Modları (Datagram) Taşıma Katmanı Güvenliği

7. Sonuç

Sis bilişim ile ilgili birçok sorunun temeli, her yerde bağlantı ve heterojen organizasyon nedeniyle ortaya çıkmaktadır. Bunun nedeni, sis ortamlarında bulunan cihazların heterojen olmasıdır. Sis bilişim, bulut hiyerarşisinin ön ucudur ve bu nedenle belirli uygulamalara göre farklı güvenlik standartlarına ihtiyaç duyar. Farklı uygulamaların farklı güvenlik gereksinimlerinin olması çözüm sürecini karmaşık ve zor hale getirir. Güvenlik tehditleri, mevcut ve ağda kullanılan protokollere göre değişir.

Makale, farklı cihaz ve farklı güvenlik protokollerinden oluşan ve henüz gelişim aşamasında olan sis bilişim mimarisinin karşılaşacağı güvenlik tehditleri ve zorlukları esas alınarak teknik ve kapsamlı bir güvenlik analizini ortaya koymuştur. Ayrıca her bir başlık altında gelişmekte olan sis platformu için güvenlik analizine ilave olarak yazılımsal veya donanımsal güvenlik önerileri sunulmuştur. Bu bağlamda sürekli gelişen teknoloji ve çeşitli protokoller, güvenli sis sistemini gerçekleştirmek ve IoT'nin güvenliğini sağlamak için standartlar geliştirilmeli ve uygulanmalıdır.

Kaynaklar

[1] Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the internet of things. ACM 2012 In: workshop on Mobile cloud computing; MCC'12, August 17, 2012, Helsinki, Finland: pp. 13-15.

[2] Suo H, Wan J, Zou C, Liu J. Security in the Internet of Things: A Review. in Proc. of IEEE 2012 International Conference on Computer Science and Electronics Engineering; March 2012, pp. 648-651.

[3] Tewari A, Gupta BB. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems 2018, pp.909-920.

[4] Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: Vision, applications and research challenges. Ad hoc networks 2012; 10(7): 1497-1516.

[5] Puthal D, Nepal S, Ranjan R, ChenJ. Threats to networking cloud and edge datacenters in the internet of things. IEEE Cloud Computing 2016;3(3): 64-71.

[6] Farooq MU, Waseem M, Khairi A, Mazhar S. A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications 2015; 11(7): 1-6.

[7] Swamy SN, Jadhav D, Kulkarni N. Security threats in the application layer in IoT applications. IEEE 2017 in Proc. International Conference on IoT in Social, Mobile, Analytics and Cloud; 10-11 Feb. 2017; Palladam, India: IEEE. pp. 477-480.

[8] Granjal J, Monteiro E, Silva JS. Security for the internet of things: a survey of existing protocols and open research issues. Surveys & Tutorials 2015; 17(3): 1294-1312.

[9] Xu LD, He W, Li S. Internet of things in industries: A survey. IEEE Transactions on Industrial informatics 2014; 10(4): 2233-2243.

[10] Al Hamid HA, Rahman SMM, Hossain MS, Almogren A, Alamri A. A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog computing Facility with Pairing-Based Cryptography. IEEE Access 2017; 5: 22313-22328.

[11] Elmisery AM, Rho S, Botvich D. A Fog Based Middleware for Automated Compliance with OECD Privacy Principles in Internet of Healthcare Things. IEEE Access 2016; 4: 8418-8841.

[12] Moosavia SR, Gia TN, Nigussie E, Rahmania AM, Virtanen S, Tenhunena H, Isoaho J. Endto-end security scheme for mobility enabled healthcare Internet of Things. Future Generation Computer Systems 2016; 64: 108-124.

[13] Liu X, Deng RH, Yang Y, Tran HN, Zhong S. Hybrid Privacy-preserving Clinical Decision Support System in Fog-cloud Computing. Future Generation Computer Systems 2018; 78: 825-837.

[14] Tang B, Chen Z, Hefferman G, Pei S, Wei T, He H, Yang Q. Incorporating Intelligence in Fog computing for Big Data Analysis in Smart Cities. IEEE Trans. on Industrial Informatics 2017; 13(5): 2140-2150.

[15] Molina B, Palaub CE, Fortino G, Guerrieri A, Savaglio C. Empowering smart cities through interoperable Sensor Network Enablers, in Proc. of 2014 IEEE International Conference on Systems, Man and Cybernetics (SMC); 5-8 Oct. 2014; San Diego, CA, USA: IEEE. pp.7-12.

[16] Cicirelli F, Guerrieri A, Spezzano G, Vinci A. An edge-based platform for dynamic Smart City applications. Future Generation Computer Systems 2017; 76: 106-118.

[17] Mohanty SP, Choppali U, Kougianos E. Everything You wanted to Know about Smart Cities. IEEE Consumer Electronics Magazine (CEM) 2016; 5(3): 60-70.

[18] Li Z, Zhou X, Liu Y, Xu H, Miao L. A Non-Cooperative Differential Game-Based Security Model in Fog computing. China Communications 2017; 14(1): 180-189.

[19] Sharma V, Lim JD, Kim JN, You I. SACA: Self-Aware Communication Architecture for IoT Using Mobile Fog Servers. Mobile Information Systems 2017; 1-17.

[20] Premarathne US, Khalil I, Atiquzzaman M. Secure and reliable surveillance over cognitive radio sensor networks in smart grid. Pervasive & Mobile Computing 2015; 22(C): 3–15.

[21] Yaakob N, Khalil I, Kumarage H, Atiquzzaman M, Tari Z. By-passing infected areas in wireless sensor networks using BPR. IEEE Transactions on Computers 2015; 64 (6): 1594–1606.
[22] Hu P, Ning H, Qiu T, Song H, Wang Y, Yao X. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. IEEE Internet of Things Journal 2017; 4(5): 1143-1155.
[23] Qiu T, Zhao A, Xia F, Si W, Wu DO. Rose: Robustness strategy for scale-free wireless sensor networks.IEEE/ACM Transactions on Networking 2017; 25(5): 2944-2959.
[24] Lee K, Kim D, Ha D, Rajput U. On security and privacy issues of fog computing supported internet of things environment, in: International Conference on the Network of the Future 2015; 1–3.
[25] Özkaynak F. Sosyal Güvenlik Kurumu Biyometrik Kimlik Doğrulama Sisteminin Problemleri ve Olası Çözüm Önerileri. Fırat Üniv. Müh. Bil. Dergisi 2016; 28(2): 185-188.