DEÜ FMD 25(75), 551-558, 2023

Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi
Dokuz Eylul University Faculty of Engineering Journal of Science and Engineering

Basılı/Printed ISSN: 1302-9304. Elektronik/Online ISSN: 2547-958X

Endüstriyel Nesnelerin İnterneti Uygulamaları için FPGA Destekli ve Bağlam Tabanlı Erişim Kontrol Güvenlik Sistemi

FPGA supported and Context-Based Access Control Security System for Industrial IoT Applications

Ahmet Tuncay Ercan [1*], Didem Genç [2], Emrah Tomur [3]

[1] Yönetim Bilişim Sistemleri Bölümü, Uygulamalı Bilimler Yüksekokulu, Yaşar Üniversitesi, İzmir, TÜRKİYE
[2] Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, İzmir Yüksek Teknoloji Enstitüsü, İzmir, TÜRKİYE
[3] Ericsson, İzmir, TÜRKİYE
Sorumlu Yazar / Corresponding Author *: tuncay.ercan@yasar.edu.tr

Geliş Tarihi / Received: 29.09.2022
Kabul Tarihi / Accepted: 16.12.2022
Araştırma Makalesi/Research Article
DOI:10.21205/deufmd.2023257503
Atıf şekli/ How to cite: ERCAN , A.T., GENÇ, D.,TOMUR, E. (2023). Endüstriyel Nesnelerin İnterneti Uygulamaları için FPGA Destekli ve Bağlam Tabanlı Erişim Kontrol Güvenlik Sistemi. DEUFMD, 25(75), 551-558.

Öz

Endüstri 4.0 ile birlikte üretimin her alanında gittikçe artan bilgisayar destekli sistemlerin yarattığı farklı ve karmaşık ağ topolojileri, artan veri miktarı, firmaların güvenlik ihtiyaçlarını artırmaktadır. Bundan dolayı farklı endüstriyel sektörlerde kullanılan farklı cihaz ve veri kullanımı şirketler, kendi kritik akıllı üretim sistemlerine yönelik güvenilir bir risk yönetim sistemine ihtiyaç duymaktadır. İşletmeler bu yüzden sahip oldukları Endüstriyel Kontrol ve Bilişim Sistemlerini korumayı amaçlarlar. Bu çalışmada üretim alanında kullanılabilecek, endüstriyel cihazlar ve/veya bunlara bağlı sensörlerin erişim kontrolü bağlamında güvenlik ihtiyaçlarını karşılayacak ve kenar bilişim kapsamında çalışacak FPGA (Alanda Programlanabilir Kapı Dizileri) destekli bir güvenlik platformu tasarlanmış ve çalışma yöntemi açıklanmıştır. Akıllı üretim cihazlarının bulunduğu bir imalathane ortamında çalışan cihaz, sensor, akıllı kontrol kutusu ve ağ geçidi gibi bileşenler üzerinde bağlam-tabanlı bir erişim denetim sistemi kullanımı gösterilmiş ve örnek bir çoklu kimlik doğrulama yöntemi tasarlanmıştır.

Anahtar Kelimeler: *Endüstri 4.0, Endüstriyel Nesnelerin İnterneti, Bağlam-Tabanlı Erişim Kontrolü, Kenar Bilişim, FPGA*

Abstract

Different and complex network topologies and increasing amount of data created by computer-aided systems within Industry 4.0 influencing every field of production, have increased the cyber security demand of companies. Therefore, companies that use different devices and data in different industrial sectors, need a reliable risk management system in their critical smart production systems. Businesses aim to protect their own Industrial Control and Information Systems. In this study, an FPGA (Field Programmable Gate Array) supported security platform that can be used in the production area, that can be used for security needs in the context of access control of industrial devices and/or sensors connected to them, and that will work within the scope of edge computing, is designed and its working method is explained. The use of a context-based access control system on the components such as smart production devices, sensors, smart control boxes and gateways operating in a workshop environment, is demonstrated with a design of exemplary multiple authentication methods.

Keywords: *Industry 4.0, Industrial Internet of Things, Context-based Access Control, Edge Computing, FPGA.*

1. Giriş

Endüstri 4.0 ile farklı sektörlerdeki fiziksel nesneleri, insanları, akıllı makineleri, üretim hatlarını ve işletme süreçlerini etkin bir şekilde kontrol edip yönetebilmek için, internet ve gömülü sistemler gibi destek teknolojileri bir araya getirilmişlerdir [1]. Nesnelerin interneti (IoT) teknolojilerinin, günümüzde yaygın bir şekilde benimsenmesi ile birlikte en iyi IoT uygulama alanlarına ilişkin 2020 yılında yapılan analizde, üretim ve endüstri %22 ile en başta olup bunu %15 ile Ulaştırma ve Mobilite, %14 ile Enerji projelerinin izlediği belirtilmiştir. Endüstriyel IoT (IIoT), Bilgi Teknolojileri (BT) ve Operasyonel Teknolojiler (OT) ile birlikte üretim ekipmanları ve ağ ortamındaki sensörleri de kullanabilen bir sistemle bütün işletme süreçlerine ve yönetimine zeka katmıştır [2].

Bu yeni nesil endüstri, üretimin her alanında daha fazla esneklik vaadinde bulunmuştur. Daha iyi kalite ve gelişmiş üretkenlik için kullanılan IIoT çözümleri, siber-fiziksel sistemler (CPS'ler), bulut gibi temel teknolojileri de dikkate alarak kullanılan bilgi işlem, büyük veri analitiği (BDA), ve bilgi-iletişim teknolojileri (BİT) ile akıllı üretim mümkün kılınmaktadır [3].

Ancak kuruluşların, iş hedefleri doğrultusunda rekabet avantajı elde edip, müşteri ve iş ortakları ile bağlılıklarını sürdürebilmeleri için, BT altyapısının tamamı üzerinde ve Endüstriyel Kontrol Sistemleri'nde kullanılan bileşenlerin ve bu sistemler üzerindeki mevcut tehditler, zafiyetler ve risklerin neler olduğunun tanımlanması ve yeterli güvenlik yöntemlerinin uygulanması gereklidir [4]. Mevcut endüstriyel iletişim sistemlerinin artan teknolojiyle birlikte kablolu/kablosuz yerel ağ alternatifleri de artmıştır. Üretim verisinin de oldukça kritik olduğu düşünüldüğünde özellikle kablosuz cihaz ve sensör kullanımının güvenlik bağlamında son derece dikkatli planlanması gereklidir [5]. Gelişen teknolojiyle birlikte tesislerin süreç ve güvenlik kontrolleri günümüzde kolaylaşmış, özellikle kritik sistemlerde EKS (Endüstriyel Kontrol Sistemi) ve SCADA (Merkezi Denetleme Kontrol ve Veri Toplama) gibi kontrol ve yönetim sistemleri oluşturulmuştur.

Sensörler ve diğer akıllı cihazlar için IoT, dijitalleştirme ve ağlara bağlanabilmeyi basitleştirip, verilerin toplanmasını ve iletilmesini kolaylaştırırken, bilgisayar korsanlarının ağlara girmesini ve zarar vermek için sensörleri kullanmasını da kolaylaştırmaktadır. BT sistemlerinde karşılanması gereken genel güvenlik fonksiyonlarının yanında, akıllı üretim sistemlerinde emniyet, güvenilirlik ve anomali tespiti gibi daha kapsamlı bir risk anlayışının uygulanması gereklidir. Bundan dolayı özellikle endüstriyel sektörler için üretimin potansiyel olarak tehdit edilebileceği, güvenlik ve çevre olayları yaratabileceği veya fikri mülkiyetin çalınabileceği endişeleri oldukça geçerli temel riskler haline gelmiştir.

Üretim sistemlerinin farklı özellikleri, akıllı cihazların çeşitliliği, kullanılan eski cihazların sayısı ve kendi içlerindeki karmaşık etkileşimleri, kullanıcı (operatörler ve mühendisler) tarafından yapılan müdahaleler, sistemlerin güvenlik gereksinimlerini farklı kılmaktadır. Akıllı bir üretim sisteminde veri sağlayan bütün cihazlara ilişkin kimlik kontrolü ve erişim yönetimi başta olmak üzere, diğer siber güvenlik riskleri dikkatle izlenmelidir. Böylece endüstriyel ağ yapısı, mevcut cihaz durumu, iletişim şekilleri, operasyonel kurallar ve olası hassasiyetler analiz edilerek gerekli tedbirler alınabilir [6], [7].

Endüstriyel güvenlik esas olarak bir yönetim sorunu olup, hali hazırda bütün güvenlik problemlerine çözüm getiren, bütünleşik bir endüstriyel siber güvenlik sistemi mevcut değildir. Böyle bir sistem ise farklı aşamalarla etkinliği arttırılan ve kullanıma hazır hale getirilerek, devamlı güncellenen ve geliştirilen güvenlik süreci demektir [4]. Endüstriyel ortamdaki üretim cihazları ve bunlara bağlı sensörlerden alınan verilerin toplanması, işlenmesi ve gerekiyorsa bir yönetim kararı verilmesi günümüzde yaygın olarak kullanılmakta olan PLC (Programlanabilir Mantık Kontrolü) denilen mikroişlemci tabanlı endüstriyel otomasyon cihazları aracılığıyla yapılmaktadır. Gelişen teknoloji ile birlikte bu cihazlarda toplanan veriler büyümekte ve işlemler karmaşık bir hal almaktadır. Daha yüksek işlemci gücü ve hafızası olan kontrol üniteleri ile programlanabilen modeller, çok daha ileri seviye getirilecek ve endüstriyel yönetim ve güvenlik ihtiyaçları doğrultusunda özel olarak geliştirilebileceklerdir. Buna ilişkin katmansal bir mimari yapı aşağıda çizilen Şekil 1'de gösterilmiştir.

5	Uygulamalar	Uygulama destekli, Görsel yazılımlar
4	Güvenlik Yönetimi	Erişim ve Veri Bütünlüğü Kontrolu
3	Ağ Yönetimi	BT ve OT sistemleri Entegrasyonu
2	Ağ Bağlantıları	Kablolu/Kablosuz Erişim ve Merkezi Bağlantı Noktaları (PLC)
1	Endüstriyel Ortam	Üretim Cihazları ve Kullanılan Sensörler

Şekil 1. Endüstriyel Üretim Sistemleri Yönetim Katmanları

Figure 1. Management Layers of Industrial Production Systems

Bu çalışmanın literatüre katkıları aşağıda maddeler halinde verilmiştir:

- Endüstriyel cihazların FPGA erişimleri esnasında güvenliği kontrol edebilmek için operasyon tabanlı erişim denetim yöntemi ile çoklu kimlik doğrulama yöntemleri birleştirilerek Endüstriyel Nesnelerin İnterneti uygulamalarına uygun bir erişim kontrol yöntemi geliştirilmiştir.
- Dinamik ve granülaritesi yüksek bir erişim denetimi sağlamak için bağlam bilgisi kullanılmıştır.
- Operasyon-tabanlı erişim denetim modelinin bir üretim senaryosu üzerinden örnek kullanımı verilmiş ve modelin doğrulaması formal olarak yapılmıştır.
- Çok katmanlı güvenlik mimarisi endüstriyel üretim sistemlerine uyarlanmıştır.

Bir sonraki bölümde endüstriyel ortamlardaki kenar bilişim ve yapay zekâ kullanımları irdelenmiş, üçüncü bölümde önerilen güvenlik altyapısı tanıtılmış ve FPGA tabanlı bir mimari model önerilmiştir. Modelde Operasyon-tabanlı Çok-katmanlı Kimlik Doğrulama Yöntemini içeren erişim kontrol mekanizması açıklanmış ve formal doğrulaması verilmiştir. Dördüncü ve son bölümde uygulama sonuçları değerlendirilmiş, ve gelecek çalışmalar hakkında bilgi verilmiştir.

2. Mevcut Çalışmalar

IoT sistemleri kullanıldıkları ortamın gereksinimlerine bağlı olmakla birlikte çok sayıda bileşeni içerdiği için doğal olarak her bir giriş noktası sibergüvenlik için tehdit demektir [8]. IoT cihazları ayrıca genel olarak şifrelenmeyen verilerin transferi, emniyetli olmayan web arayüzleri, düşük seviyeli yazılım korumaları ve yetersiz yetkilendirilme gibi güvenlik hassasiyetleri ile bilinmektedir [9]. IIoT, fabrikalardaki kritik üretim sistemlerini nasıl izleyebileceğimiz konusunda akıllı sensörlerin desteğiyle büyük değişiklik getirmiştir.

Üretim ortamında kullanılmakta olan akıllı tezgâhlardan, robotlara ve ortam verisi sağlayan sensör ve uygun reaksiyon gösteren tümleşik cihazlara kadar, hemen hemen bütün bileşenler için, siber güvenlik isteğe bağlı değil, bir gerekliliktir. Referans [10]'de M2M (Makineler Arası İletişim) sistemleri için geliştirilen hibrit güvenlik yapılarında, katmansal yönetim ve güvenlik mimarileri önerilmiştir. M2M sistemler, internet dünyası için yeni riskler doğurmamakla birlikte mevcut tehlike ve risklerin boyutunu arttırmıştır [11].

Başka bir yüksek lisans tez çalışmasında özellikle düşük kapasiteli gömülü cihazların IoT sistemi içerisine dahil edilmesiyle, ağlar üzerindeki veriler TLS (Taşıma Katmanı Güvenliği) ile güvenli olarak transfer edilebilmektedir [12]. Güvenli cihaz kimlik doğrulaması, Nesnelerin İnternetinin çok önemli bir yönüdür ve kimlik sağlama, kimlik doğrulama ve erişim kontrolü gibi birbirini takip eden güvenli aşamalardan oluşmaktadır.

Akıllı üretim sistemlerindeki sibergüvenlik fonksiyonları için ilk akla gelen erişim kontrol tedbirleri uygun yetkilendirme ve davranış analizleriyle engellenebilir.

Bu şekildeki güvenlik açığı taramaları, BT sistemlerini zayıflıklara karşı kontrol edebilen otomatik süreçlerdir. Güvenlik açığı tarayıcısı, verileri mevcut ağ bağlantısı üzerinden test edilecek sisteme iletir. Aldığı yanıtlar, bir güvenlik açığı veritabanı kullanılarak değerlendirilir ve zayıflıklar açısından kontrol edilir. Sızma testi gibi riske dayalı süreçlerin aksine, güvenlik açığı taramaları kapsamlı testlere odaklanmıştır .

Bizim bu çalışmadaki amacımız da üretim ortamında kullanılmakta olan IIoT cihazlarını ve/veya bu cihazlara bağlı sensörlerin erişiminde güvenliği sağlamaktır. Bu amaçla operasyon tabanlı erişim denetim yöntemini çoklu kimlik doğrulama ile birleştirerek arttırılmış dinamik bir güvenlik sistemi geliştirilmiştir.

3. Önerilen Güvenlik Altyapısı

Endüstriyel otomasyon ve kontrol sistemleri standart yazılım ve donanım bileşenlerinden oluşmaktadır. Bu açık sistemler birlikte çalışmayı kolaylaştırırken, sistemleri saldırılara, sabotajlara ve casusluk gibi farklı güvenlik tehditlerine karşı savunmasız duruma getirir. Endüstriyel iletişim ağları için riski azaltmayı amaçlayan uluslararası IEC 62443 standardı, siber güvenlik için doğru yapılandırılmış bir yaklaşım sağlar [13]. Endüstri 4.0'da kullanılan siber-fiziksel sistemler (CPS), yakın gelecekte muhtemelen en önemli teknolojik gelişmelerden biri haline gelecektir. Bu sistemler de makine öğrenmesi ve yapay zeka desteği ile birlikte çalışan, bütün bileşenlerinin maksimum verimliliğe çıkarıldığı, bilgisayar yazılımları tarafından kontrol edilen fiziksel yapılardır [14].

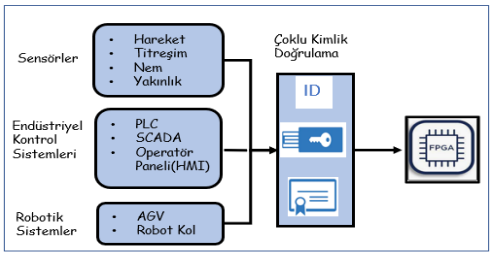
Bu amaçla kullanılabilecek işlem kapasitesine sahip farklı tümleşik devreler (SoC- System on Chip) daha düşük maliyetlerle sağlanabilmelerine rağmen, FPGA'ler tasarımcının ihtiyaç duyacağı bütün fonksiyonları gerçekleştirilebilme kolaylığından dolayı daha esnek ve kullanışlıdır [15].

Endüstriyel ağların kısmi kontrol noktası olan PLC sistemlerinin yerine kullanılacak FPGA tabanlı akıllı kontrol kutuları, geleneksel bir ağdaki anahtar yapılar gibi VLAN (Virtual Local Area Network) ağlarına benzer şekilde erişim izinlerini (access list) kontrol edebilir. Üretim ortamındaki sensör cihazları ve üretim ekipmanı gibi bütün veri uç noktaları kötü niyetli işlemlerden korunmalıdır. Ortam içinde kullanılan bütün cihazların tanımlanmış olması ve takiplerinin sağlanarak geçerli güvenlik önlemlerinin devam ettirilmesi önemlidir. Buna göre planlanması gereken faaliyetler şunlardır;

- Ağdaki bütün cihazların algılanması,
- Cihazların görev ve lokasyonlarına göre sınıflandırılması için (çalışan-çalışmayan cihazlar dahil) ayrı ayrı profillendirilmesi ve uyumluluk kontrollerinin yapılması,
- Erişim Kontrollerinin yapılması,
- Sürekli izleme ve anomali tespiti ile veri bütünlüğü kontrolü.her

3.1. Operasyon-tabanlı çok-katmanlı kimlik doğrulama yöntemi

Bir erişim denetim sisteminde, aynı aksiyon için bile farklı nesnelere erişimde farklı kimlik doğrulama metotları kullanılabilir. Örneğin, kritik bir kaynağa komut verilirken veya daha gelişmiş bir kimlik doğrulama kullanılırken, bir sensörden veri okumada yalnızca "id" kullanılarak kimlik doğrulama yapılabilir. Bu durum literatürde çok-katmanlı kimlik doğrulama olarak tanımlanmaktadır. Şekil 2'de bir üretim hattı için olabilecek çok katmanlı kimlik doğrulama örneği bulunmaktadır.



Şekil 2. Çok-katmanlı Kimlik Doğrulama

Figure 2. Multi-layered Authentication

Bu örneğe yönelik olarak belirlenmiş olan senaryo kapsamında üretim sektöründe faaliyet gösteren bir fabrika ortamında akıllı nesneler (üretime katılan akıllı cihazlar ve/veya bunlara entegre sensörler) ve FPGA, PLC ve SCADA gibi sistemlerin bulunduğu farz edilmiştir. Sensörler, EKS ve robotik sistemlerden oluşan bu üç katmanlı sisteme ilişkin kimlik doğrulama metodunun uygulanabilmesi için erişim denetim tablosuna ihtiyaç vardır. Ortamda bulunan bütün nesne ve sistemlerin önceden planlanmış çalışma fonksiyonlarına göre uygun bir erişim desteği planlaması Tablo 1'de gösterilmiştir. Tablo'da görüldüğü üzere bu erişim denetimi operasyonlar, bu operasyonlar için tanımlı nesne veya özneler, belirli nesne öznitelikleri altında gruplanmış nesneler ve ilgili bağlam bilgisinden oluşmaktadır.

Tablo 1. Örnek Senaryo Erişim Denetim Tablosu.

Table 1. Access Control Table for Sample Scenario.

Operasyon	Obje Öznitelik	Bağlam	Erişim İzini
Komut Verme FPGA PLC	AGV	Bağlam 1 ^ (Bağlam 2 V Bağlam 3)	Evet
	Robot Kol	Bağlam 1 ^ Bağlam 3	Evet
	CNC	Bağlam 1	Evet
Veri Okuma FPGA SCADA	Sensör	Bağlam 1 ^ Bağlam 2	Evet
	PLC	Bağlam 1	Evet

Senaryo ortamında temel olarak komut verme ve veri okuma operasyonları bulunmaktadır. Her operasyonun altında bu operasyonu

gerçekleştirebilecek nesne veya özneler görülmektedir. Bağlam sütununda ilgili nesne üzerinde ilişkili operasyonu gerçekleştirebilmek için sağlanması gereken bir veya birden fazla bağlam şartı sıralanmıştır. Bağlamlar çoklu kimlik doğrulama yöntemi, ortam sıcaklığı, lokasyon, zaman gibi çevresel veya özel tanımlı, o ortam için anlamlı özelliklerdir. Örneğin; buradaki senaryo için Bağlam1, çoklu kimlik doğrulamayı nitelemekte, ve AGV(Otomatik yönlendirmeli Araç) 'ye komut vermede sertifika istenirken, CNC(Sayısal Kontrollü Bilgisayar)'ye komut vermede yalnızca id ile kimlik doğrulama yeterli olabilmektedir. Yani, bir FPGA cihazı AGV'ye komut verirken sertifikalı haberleşme protokolü üzerinden kimlik doğrulama olmaması halinde erişim iznine sahip olamayacaktır. Tabloya göre;

(1) PLC nesnesi erişmek istediği nesne için ilgili bağlam bilgisinin sağlanması halinde komut verme operasyonunu gerçekleştirebilir,

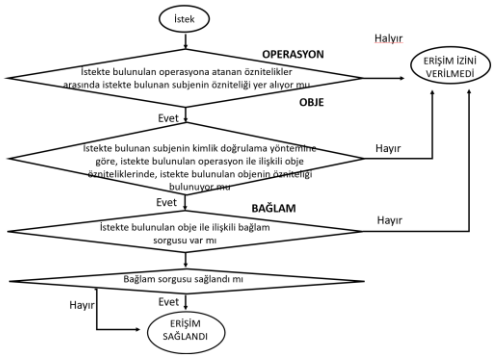
(2) SCADA nesnesi hiçbir şekilde komut verme operasyonu gerçekleştiremez, sadece veri okuyabilmektedir,

(3) Sistemdeki akıllı nesnelerimiz ise AGV, Robot Kol, CNC, PLC ve sensörlerimizdir. Nesnelerden uygun olanlar aynı nesne özniteliği altında gruplanabilmektedir. Örneğin, sensörler nesne özniteliği; hareket, titreşim ve nem sensörü gibi bir çok sensör barındırmaktadır.

(4) Bağlam bilgisi içerisinde çok katmanlı kimlik doğrulama bulunmaktadır.

3.2. Erişim kontrol yöntemi

Operasyon-tabanlı erişim denetim sisteminde erişim izinleri esas olarak operasyonlara bakılarak verilir [16]. Erişim denetiminde bulunan özne/nesnenin ilgili operasyonu gerçekleştirmek için izni olup olmadığı kontrol edildikten sonra, istekte bulunulan kaynak için ilgili operasyon üzerinde tanımlı bağlam bilgisi olup olmadığı kontrol edilir. Bağlam bilgisinin sağlandığı durumda erişim izini verilir. Operasyon-tabanlı erişim denetim sistemini anlatan akış diyagramı Şekil 3'te verilmiştir.



Şekil 3. Operasyon-tabanlı Erişim Kontrolü Akış Diyagramı [17]

Figure 3. Flow Diagram of Operation based Access Control [17]

3.3. Doğrulama

Önerilen erişim denetim sisteminin formal doğrulaması aşağıda detaylı olarak verilmiştir.

Tanım 1. Varlıklar

Bu erişim denetim modelinde 3 adet varlık bulunmaktadır:

1. Operasyonlar: Operasyonlar nesneler üzerinde alınabilecek aksiyonlar kümesidir. Özne öznitelikleri operasyonlara göre gruplandırılmaktadır. Operasyonlar "Op" kısaltması ile gösterilmektedir.

2. Özneler: Erişim denetim modelinde bir nesne üzerinde aksiyon almaya izinli herhangi bir varlıktır. Uygulamalar, cihazlar, kullanıcılar, prosesler özne olarak sayılabilir. Özneler "S" kısaltması ile gösterilmiştir.

3. Nesneler: Belirli kurallar dahilinde erişime açık olan her kaynak nesne olarak sayılabilir. Nesneler "O" kısaltması ile gösterilmiştir.

Tanım 2. Bağlam Kuralları

Bağlam: Bağlam bilgisi bir nesneye erişimde kullanılabilecek her türlü kısıtlama olarak tanımlanabilir. Örneğin; bu çalışmada çoklu kimlik doğrulama bir bağlam bilgisi olarak kullanılmıştır. Bağlam bilgisinin resmi gösterimi aşağıdaki gibidir:

<BağlamAdı,Operatör,Değer> **(1)**

Bağlam Kuralları: Bağlam kuralları bir isteğin sonucunun izin mi yoksa ret mi olacağını gösteren formal ifadelerdir. Bağlam kuralı bağlam ve aksiyon olarak iki parçadan oluşmaktadır. Bağlam kuralları kümesi "***CR***"

kısaltması ile gösterilmiş olup, aşağıda örnek bir bağlam kuralı verilmiştir.

CRi = <(BağlamAdı,Operatör,Değer), Aksiyon> CRi ϵCR (2)

Nesne öznitelik sistem yöneticisi veya üretici tarafından nesneye tanımlanan, nesnenin özelliklerini belirten bir etikettir. Her nesnenin en az bir nesne özniteliği bulunmak zorundadır. "OA" nesne özniteliğin kısaltmasıdır.

Tanım 3. Atama İlişkileri

Özne-özne özniteliği ve nesne-nesne özniteliği arasındaki ilişki aşağıdaki gibi ifade edilebilir:

- **SSAa ⊂ S x SA**, bir özne birden çok özniteliğe sahip olabileceği gibi, bir öznitelik birden çok özneye atfedilmiş olabilir.
- **OOAa ⊂ O x OA**, bir nesne birden çok özniteliğe sahip olabileceği gibi, bir öznitelik birden çok nesneye atfedilmiş olabilir.
- **SAOpa ⊂ SA x Op**, özne özniteliği ve operasyon arasındaki çoklu ilişkiyi tanımlar.
- **OAOpa ⊂ OA x Op**, nesne özniteliği ve operasyon arasındaki çoklu ilişkiyi tanımlar.
- **CROAa ⊂ CR x OA**, bağlam kuralları ve nesne özniteliği arasındaki çoklu ilişkiyi tanımlar.

Tanım 4. Varlık Ataması

- Bir **sa ϵ SA** ise ;
  atanmış_özne (sa) = {s ϵ S | (s,sa) ϵ SSAa};
  sa özne özniteliğine atanmış olan bir özne kümesini tanımlar.
- Bir **oa ϵ OA** ise;
  atanmış_nesne(oa)={o ϵ O | (o,oa) ϵ OOAa};
  oa nesne özniteliğine atanmış olan bir nesne kümesini tanımlar.
- Bir op ϵ Op ise;
  atanmış_özne_öznitelik (op) = {sa ϵ SA | (sa,op)ϵ SAOpa} ;
  op operasyonuna atanmış özne özniteliği kümesini tanımlar.
- Bir op ϵ Op ise;
  atanmış_nesne_öznitelik (op) = {oa ϵ OA | (oa,op) ϵ OAOpa};
  op operasyonuna atanmış nesne özniteliği kümesini tanımlar.
- Bir oa ϵ OA **ise;**
  ilişkili_bağlam_kuralı (oa) = {cr ϵ CR | (cr,oa) ϵCROAa};
  oa nesne özniteliği ile bağıntılı olan bağlam kuralını tanımlar.
- Bir cs ϵ CS ise;
  aktif_bağlam={cr ϵ CR | (cr,1)};
  bağlam kuralı sağlanmış olan (aktif) kuralları tanımlar.

Yukarıda verilen bilgiler göz önünde bulundurulduğunda Şekil 4.'te verilen formal ifadeyi elde ederiz.

(∀op: Operasyon) (∀s: Özne) (∀o: Nesne):

İZİN(s,o,op)⇒

(∃sa: Özne öznitelik) (∃oa:Nesne Öznitelik)(∃s: Özne)(∃o: Nesne):

[op ϵ Op ^ s ϵ atanmış_özne(sa) ^ o ϵ atanmış_nesne(oa) ^

sa ϵ atanmış_özne_öznitelik(op) ^ oa ϵ atanmış_nesne_öznitelik(op)]

^ [ilişkili_bağlam_kuralı(oa) = ∅ ˅ ilişkili_bağlam_kuralı ϵ aktif_bağlam]

Şekil 4. Formal İfade Formülü

Figure 4. Formal Expression Formula

4. Sonuç

Bu çalışma kapsamında endüstriyel ortamda akıllı ağ geçidi ve akıllı PLC olarak kullanılabilecek FPGA cihazları üzerinde çalışan çok katmanlı kimlik doğrulama sunan bağlam-tabanlı bir erişim kontrolu güvenlik sistemi tasarlanmıştır.

İşletmelerin kendi üretim sistemlerindeki IIoT bağlantılı cihazlar için yapılandırılacak yönetim ve güvenlik platformları operasyonel verimlilikleri için oldukça önemlidir. Bu çalışmada üretim ortamındaki endüstriyel cihazların, ortam ve cihaz üzerine monte edilmiş sensörlerin, bilgi sistemlerine ait bütün bileşenlerin güvenilir olarak nasıl biraraya getirileceği ile ilgili şu problemlere çözüm getirilmiştir:

- Sistemin mantıksal yapılandırılması, bütün bileşenlerin operasyon, özne ve nesne tanımlamalarının yapılması,
- Cihaz ve veri iletiminin sisteme nasıl dahil edileceği,
- Bağlam-tabanlı kuralların belirlenmesi ve varlık atamaları,
- Operasyon-tabanlı çok katmanlı kimlik doğrulama yönteminin bahsi geçen üretim ortamları özelinde örnek bir senaryo ile kullanımının gösterilmesi,

Bu çalışmadaki plastik enjeksiyon kalıp imalathaneleri için tasarımı yapılan FPGA destekli ve bağlam tabanlı erişim kontrol sistemi

bu senaryonun dışında bütün endüstriyel imalat sektörlerinde kullanılabilir. FPGA tümleşik devresinin tekrar tekrar yapılandırılabilmesi, yeni sistem bileşenleri açısından esnek bir güncelleme imkanı verecektir. Ayrıca ağ ve uygulama katmanlarında bu yapıyı daha da etkinleştirebilecek yazılım tabanlı ağ yönetim ve güvenlik çözümleri (Yazılım Tanımlı Ağ (SDN) ile Ağ Fonksiyonlarının Sanallaştırılması (NFV) vb.) teknolojileri de kullanılabilir.

5.Conclusion

In this research, a security system that offers context-based access control with multi-layered authentication was developed, suitable for deployment on FPGA devices functioning as smart network gateways and smart PLCs in industrial settings.

Setting up effective management and security platforms for IIoT-connected devices within their production systems holds paramount importance for operational efficiency in enterprises. The study addresses the following challenges concerning the reliable integration of industrial devices, environment sensors, and information system components:

- Organizing the system logically, including defining the operation, subject, and object identifications for all elements.
- Incorporating device and data transmission seamlessly into the system.
- Establishing context-based rules and entity assignments.
- Demonstrating the practical application of the operation-based multi-layered authentication method through a sample scenario tailored to specific production environments.

The FPGA-supported context-based access control system designed for plastic injection mold manufacturing can be adapted to various industrial manufacturing sectors. The reconfigurable nature of FPGA integrated circuits allows for flexible updates with new system components. Moreover, the use of software-based network management and security solutions, like Software-Defined Networking (SDN) and Network Function Virtualization (NFV), could further enhance this framework at the network and application levels.

Etik kurul onayı ve çıkar çatışması beyanı

Hazırlanan makalede etik kurul izni alınmasına gerek yoktur. Hazırlanan makalede herhangi bir kişi/kurum ile çıkar çatışması bulunmamaktadır.

Kaynakça

[1] Schumacher, A., Erol, S., & Sihn, W. 2016. A maturity model for assessing Industry 4.0 readiness and maturity of manufacturing enterprises. Procedia Cirp, Cilt. 52, s. 161-166. DOI: 10.1016/j.procir.2016.07.040

[2] IoT Analytics, Market Insight for the Internet of Things. https://iot-analytics.com/top-10-iot-applications-in-2020 (Erişim Tarihi: 09.08.2022)

[3] R.Y. Zhong, X. Xu, E. Klotz, S.T. Newman. 2017. Intelligent manufacturing in the context of industry 4.0: A review, Engineering 3, 616–630. DOI: 10.1016/J.ENG.2017.05.015

[4] BTK Akademi, Endüstriyel Kontrol Sistemlerinin Siber Güvenliği. https://www.btkakademi.gov.tr/portal/course/enduestriyel-kontrol-sistemlerinin-siber-guevenligi-20792. (Erişim Tarihi: 09.08.2022)

[5] Ercan,T. 2005. Modeling and Designing Wireless Networks for Corporations: Security Policies and Reconfiguration. Dokuz Eylul University, Graduate School of Natural and Applied Sciences, PhD Thesis.

[6] Lu, Y. 2017. Industry 4.0: A survey on technologies, applications and open research issues, Journal of industrial information integration, Cilt. 6, s. 1-10. DOI: 10.1016/j.jii.2017.04.005

[7] Qin, J., Liu, Y., & Grosvenor, R. 2016. A categorical framework of manufacturing for industry 4.0 and beyond., Procedia cirp, Cilt. 52, s. 173-178. DOI: 10.1016/j.procir.2016.08.005

[8] 9 Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. 2015. On the security and privacy of Internet of Things architectures and systems, In 2015 International workshop on secure internet of things (SIoT), 49-57. DOI: 10.1109/SIOT.2015.9

[9] Lee, I., & Lee, K. 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business horizons, Cilt. 4, s. 431-440. DOI: 10.1016/j.bushor.2015.03.008

[10] Polat, H., & Oyucu, S. 2017. Token-based authentication method for M2M platforms. Turkish Journal of Electrical Engineering and Computer Sciences, Cilt. 25, s. 2956-2967. DOI: 10.3906/elk-1608-6

[11] Barki, A., Bouabdallah, A., Gharout, S., & Traore, J. 2016. M2M security: Challenges and solutions. IEEE Communications Surveys & Tutorials, Cilt. 18, s. 1241-1254. DOI: 10.1109/COMST.2016.2515516

[12] King, J. 2015. A Distributed Security Scheme to Secure Data Communication between Class-0 IoT Devices and the Internet, Master Thesis, 2015, Sweden.

[13] IEC 62443. The Ultimate Guide to Protecting OT Systems with IEC. https://verveindustrial.com/lp/iec-62443-whitepaper/ (Erişim tarihi: 09.08.2022)

[14] Chen, H. 2017. Applications of cyber-physical system: a literature review. Journal of Industrial Integration and Management, 2(3), s.1750012 (28 pages). DOI: 10.1142/S2424862217500129

[15] Ercan, T., Al Azzawi, AK. (2019). Design of an FPGA-based Intelligent Gateway for Industrial IoT. International Journal of Advanced Trends in Computer Science and Engineering. Volume 8, No.1.2, 126-130.

[16] Genç, D., Tomur, E., & Erten, Y. M. 2019. Context-Aware Operation-Based Access Control for Internet of Things Applications. In 2019 International Symposium on Networks, Computers and Communications (ISNCC), s. 1-6. DOI: 10.1109/ISNCC.2019.8909196

[17] Genç, D. 2018. Context aware role based access control model for internet of things applications .İzmir Yüksek Teknoloji Enstitüsü, Mühendislik ve Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 23s, İzmir.