IJMSIT

International Journal of Multidisciplinary Studies and Innovative Technologies

Volume : 3
Number: 1
Year: 2019
Pages: 56 - 65

Makineler Arası İletişim Sistemlerinde Güvenli Veri Aktarımı İçin Bir Hibrit Güvenlik Şema Önerisi

Cihan BAYRAKTAR[1*], Hadi GÖKÇEN[2]

[1]*Bilgi Güvenliği Teknolojileri Programı / Eskipazar Meslek Yüksekokulu, Karabük Üniversitesi, Karabük*
[2]*Endüstri Mühendisliği Bölümü / Mühendislik Fakültesi, Gazi Üniversitesi, Ankara*
[*]*Corresponding author: cihanbayraktar@karabuk.edu.tr*

Özet **-** Endüstri 4.0 son zamanların en popüler konularından biri olmayı sürdürmektedir. Bünyesinde, zeki fabrika sistemleri, kendi aralarında otomatik iletişim kurarak süreci yönetebilen makineler ve ortaya çıkan zeki ürünler bulundurduğu için ilgi alanında kalmaya devam edecektir. Ancak, yeni nesil endüstri devrimi kapsamında ele alınan uygulamalar, temelde bilgisayar destekli yönetim, veri toplama ve işleme sistemleri çalıştırdıklarından dolayı siber suçlara karşı ilgi uyandırmaktadırlar. Bundan dolayı, Endüstri 4.0 gelişmelerinin önem verilmesi gereken adımlarından biri de siber güvenliktir. Çünkü, sistem içerisinde bulunan tüm parçalar internet alt yapısı ile iletişim kurmakta ve siber saldırılara karşı açık hale gelmektedir. Güvenli bir endüstri 4.0 yapısı için gerekli siber güvenlik önlemlerinin alınması şarttır. Bu sayede işletmeler kendi iç ve dış süreçlerinin aksamasını ve verimlilik kaybını engelleyebilirler. Bu çalışmada endüstri 4.0 kavramlarından olan makineler arası iletişim (M2M) sistemleri için hibrit güvenlik şeması önerilmiş ve test edilmiştir. Yapılan testler sonucunda, geliştirilen şema ile cihazlar arasında yapılan veri alışverişinin gizliliği, bütünlüğü ve güvenliğinin sağlandığı tespit edilmiştir.

Anahtar Kelimeler – Endüstri 4.0, Makineden Makineye İletişim, Bilgi Güvenliği, Hibrit Şifreleme, Veri Gizliliği

A Hybrid Security Scheme Proposal for Safe Data Transmission in Machine to Machine Communication Systems

Abstract **-** Industry 4.0 remains one of the most popular topics of recent times. Because of it has intelligent factory systems and machines that can manage the process by automatically communication among themselves, and intelligent products that arise, Industry 4.0 will remain in the area of the interest. However, the practices covered in the new generation of industrial revolution are arousing interest about cybercrime, because of they employ computer aided management, data collection and processing systems. Therefore one of the steps that should be given importance of the developments of Industry 4.0 is cyber security. Because, all parts in system communicate with infrastructure of the internet and be vulnerable against the cyber-attacks. It is essential to have the necessary cyber security measures for a safe industry 4.0 structure. In this way, businesses can prevent hitch of their internal and external processes and loss of productivity. In this study, a hybrid security scheme has been developed and have been controlled for the machine to machine communication (M2M) that is part of the industry 4.0. As a result of tests, have been determined that provide privacy, integrity and security of the data exchange among devices with developed scheme.

Keywords – Industry 4.0, Machine to Machine Communication, Information Security, Hybrid Cryptography, Privacy of Data

I. GİRİŞ

Endüstri 4.0 terim olarak, tüm endüstriyel sistem içerisin kullanılan cihazların birbirleri ile bağlantılı bir yapı içerisinde bulunmalarını temsil etmektedir. Endüstri 4.0 devrimi, zeki üretim süreçleri ile gömülü sistemlerin birleştirilmesi ile yeni bir teknolojiyi elde etmek ve devamında üretim süreçleri gibi işletme içerisindeki tüm kademelere uygulanmasını amaçlamaktadır. Günümüz işletmeleri, birçok gelişmiş ürünün üretilmesi aşamasında büyük veri yığınlarının cihazlar arasında aktarılması ve işlenmesi konusunda sorunlar yaşamaktadırlar. Yeni nesil endüstri devrimi teknolojilerinden gösterilen siber fiziksel sistemler, yaşanan bu sorunların çözümü için zeki birimleri iç içe girdiği yapılardan oluşan yapay zeka sistemleri ve büyük veri yığınlarının güvenle depolanabileceği bulut bilişim olanakları gibi imkanlar sunabilmektedir [1].

Dördüncü endüstri devrimi kapsamında değerlendirilen birçok uygulamanın temelinde, bilgisayar destekli merkezi yönetim, veri toplama ve işleme mekanizmaları bulunmaktadır. Bu mekanizmalar ile kurulan sistem, her geçen gün siber suçlara karşı ilgi odağı olmaya devam etmektedir. Bundan dolayı işletmeler, kendi iç ve dış süreçlerinin aksamasını engellemek, iş verimliliğini kaybetmemek ve sistem içerisinde üretilen ve işlenen verilerin yetkisiz kişilerin eline geçmesini engellemek için çeşitli bilgi güvenliği uygulamalarına ihtiyaç duymaktadırlar [2].

Bu çalışmada, endüstri 4.0 teknolojilerinden biri olarak gösterilen siber fiziksel sistemler kapsamındaki Makineden Makineye (M2M) veri iletişiminde üretilen, işlenen ve aktarımları yapılan verilerin, yetkisiz kişilerin eline geçmesini ve olası saldırılar sonucunda sistem içerisine gönderilecek zararlı verilerin işleme alınmasının

engellenmesi amacıyla, bir hibrit şifreleme ve kimlik doğrulama şeması önerilmiş ve kullanımı ile veri gizliliğinin ve güvenliğinin sağlanabileceği aktarılmaya çalışılmıştır. Çalışmanın ikinci bölümünde endüstri 4.0 kavramı hakkında genel bilgilendirme yapılmış, ardından üçünü bölümde bilgi güvenliği kavramı ile birlikte endüstri 4.0 teknolojilerini tehdit eden unsurlar hakkında bilgi verilmiştir. Dördüncü bölümde konu hakkında bugüne kadar yapılmış olan çalışmalar tanıtılmıştır. Beşinci ve altıncı bölümlerde ise çalışma kapsamında önerilen hibrit güvenlik şemasının tanıtımı ve uygulama sonuçları hakkında bilgiler verilmiştir.

II. ENDÜSTRİ 4.0

Dördüncü endüstri devriminin, Kagermann, Lukas, & Wahister (2011) tarafından kaleme alınmış olan makale ile başladığı belirtilmektedir [3]. Bu makaleye göre, Endüstri 4.0 otomasyondaki gelişmeler ve bunların yanında zeki gözlem ve karar verme aşamalarını da kapsadığı ifade edilmektedir [4].

Bütünleşmiş sanayi adı ile bilinen Endüstri 4.0 son zamanlarda herkes tarafından dile getirilmektedir. Büyük işletmeler, orta sınıf işletmeler ve kamunun belli kesimleri Endüstri 4.0 ile ilişkili yeni fırsatları incelemeye devam etmektedirler. Dördüncü endüstri devrimine karşı oluşan bu ilgi, sadece en önemli uluslararası bir fuar olan Hannover Fuarının odak alınmasıyla değil, ayrıca Alman hükümetine bağlı birkaç bakanlık tarafından destek sağlanan BT Zirvesindeki profilini de önemli ölçüde yükseltmiştir. Fakat sanayiyi kuşatan bu büyük yayılımda, büyük veri, bulut bilişim, siber fiziksel sistemler, RFID mimarileri, nesnelerin ve hizmetlerin interneti ve makineler arası iletişim gibi Endüstri 4.0 terimleri birçok pazarlama stratejisinin niyeti gibi özensiz bir şekilde kalmıştır. Bu düzensiz Endüstri 4.0 tanımı defalarca, sonrasında karşılaşılmayan ve hayal kırıklığına neden olan fazla abartılmış beklentilere yol açmıştır. Tedarikçileri, Endüstri 4.0 kapsamında değerlendirilen teknolojilerin, makine otomasyonunu tamamlayıcı nitelikte olduklarını ve bu sayede üretim maliyetlerinin tüketicilerin lehine daha uygun seviyelere ulaştırılabileceğini ifade etmişlerdir [5].

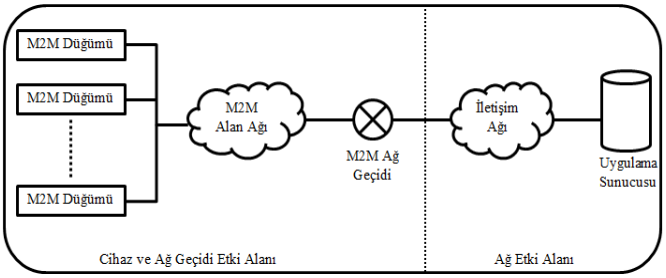
Endüstri 4.0'a ait merkezi yönler, üç paradigma ile daha net bir şekilde belirlenebilir. Bunlar; zeki ürün, zeki makine ve arttırılmış operatördür. zeki ürünün ana fikri, sistemin aktif bir bölümüne iş parçasının rolünü yaymak olarak ifade edilmektedir. Bu paradigmada ürünlerin, operasyonel verilerin ve gereksinimlerin doğrudan bir bireysel inşa planı olarak saklandığı hafızanın yerini aldığı belirtilmektedir. Yani bu durumda ürün, kendisi için gerekli kaynakları talep eden ve kendi üretim süreçlerini yönlendiren bir durum haline gelmektedir. Bu, modüler üretim sistemlerinde ürünlerin kendi kendilerini konfigüre edebilme seviyesine ulaşabilmeleri için sahip olmaları gereken ön şarttır. İkinci paradigma olan zeki makineler, makinelerin siber fiziksel sistem olma süreçleri olarak tanımlanmaktadır. Bu süreçte geleneksel üretim hiyerarşisi, siber fiziksel sistemler tarafından etkinleştirilen kendi kendine örgütlenme sistemine dönüştürülecektir. Ayrıca üretim hatları, oldukça esnek seri üretim koşulları altında, en küçük parti büyüklüğünü bile üretebilecek kadar esnek ve modüler bir seviyeye ulaşacaktır. Üçüncü paradigma olan arttırılmış operatör, modüler üretim sistemlerinin mücadeleci çevresi içerisinde çalışanlar için teknolojik destek sağlamayı hedef almaktadır. Endüstri 4.0, çalışanın olmadığı bir üretim tesisi oluşturmayı amaçlamamaktadır. Çalışanlar, giderek daha da zorlu bir ortam haline gelen iş çevresinin, azami ölçüde uyum sağlayabilen en esnek parçaları olarak kabul edilmektedirler [6].

Bu üç paradigmanın uygulanabilirliği için endüstri 4.0 kapsamında değerlendirilen siber fiziksel sistemlerin ve makineler arası iletişimin (M2M) güvenlik süreçleri dikkate alınarak kullanılması önemlidir. Yapı içerisinde bulunan siber fiziksel sistemler, fiziksel dünya ile siber dünyanın internet alt yapısı ile birbirine bağlanmasına imkan vermektedir. Bu sistemler sensörler ile donatılmışlardır ve bu sayede fiziksel dünyada gerçekleşen hareketler internet hizmetleri ile toplanmaktadır. Bunu sonucunda elde edilen veriler nesnelerin birbirleri ile etkileşimlerinde kullanılmaktadır [4].

M2M, işletme süreçlerinin yönetilmesi için sensörler ile diğer cihazların birbirlerine kablolu veya kablosuz bağlandıkları, kökeni Merkezi Denetim ve Veri Toplama (SCADA) sistemlerine dayanan yeni bir teknolojidir. Bu teknolojide ağa bağlı zeki cihazlar ile insandan bağımsız süreç kararları makineler tarafından alınabilmektedir [7].

Geliştirilen siber fiziksel sistemler sayesinde yeni nesil iş modellerinin temeli M2M sistemler tarafından oluşturulmaktadır. İşletme içerisinde çalışan makinelerin birbirleri ile bağlantılı duruma gelerek iletişim kurabilmeleri, işletme içi tüm süreçlerin uygulanma şekillerini yeniden tanımlamaktadır. M2M sistemlerin sayesinde işletmeler, çok hızlı ve etkin kararlar alabilecek ve kullanılan otomasyonun önemi daha da artacaktır. Ayrıca bu sistem, nesnelerin interneti kavramını da destekleyerek tüketici cihazları ve hizmetlerini de sistem içerisine dahil edebilecektir [8]. Tüm bu gelişmeler, yeni nesil endüstri içinde geliştirilen, üretim sistemini tamamen sensörler ve özerk sistemler ile donatılmış, her aşamada programlamanın çeşitli teknolojilerinin uygulanması ile ilişkili olan zeki teknolojileri kullanan zeki fabrikalar çatısı altında gerçekleştirilmektedir [9].

Temel anlamda M2M sistemin yapısı üç katmandan oluşmaktadır. Birinci katman, M2M sistemi içerisinde çalışan cihazlar için veriyi temin eden sunuculardır. İkinci katman iletişim katmanı olarak bilinir ve verinin transferi süreçlerinden sorumludur. Üçüncü katman ise sistemi içerisindeki cihazlardan gelen verilerin işlenmesi süreçlerinin gerçekleştirildiği uygulama katmanıdır [10]. Avrupa Telekomünikasyon Standartları Enstitüsüne göre M2M yapısı, Şekil 1' de gösterilmektedir. M2M sistemi, cihaz, ağ geçidi alanı ve ağ etki alanı olmak üzere 3 temel bileşeni içerisinde bulundurmaktadır. Cihaz ve ağ geçidi alanı bileşenleri, M2M sistemleri içerisinde kullanılan çeşitli zeki cihazlardan oluşmaktadır. M2M alan ağı, sistem içerisindeki veri iletişimi için üç tip ortam sağlamakla görevli olan bileşendir. Bu ortamlar; cihazlar arası iletişim, ağ geçitleri arası iletişim ve cihaz ile ağ geçidi arası iletişim olarak gruplandırılmaktadırlar. M2M sisteminin son temel bileşeni olan ağ etki alanı ise verinin, M2M cihazları tarafından internet altyapısı ile yine M2M uygulama sunucularına ulaştırılması ile ilgili görevleri yerine getirmektedir [11].



Şekil 1. M2M Yapısı [11].

M2M sistemler, üretkenliği ve verimliliği arttırmasının yanında maliyetleri düşürmesinden dolayı, son yıllarda insanlar ve işletmeler tarafından ilgi çekici duruma gelmiştir. Hatta gelecek ağ sistemlerinin dikkat çeken ana konularından biri olarak değerlendirilmektedir. M2M sistemlerin ilgi çeken bir başka konusu ise güvenlik karakteristiğidir. Bu sistemlerin kendisi çeşitli siber saldırılara karşı açıklara sahip olduğundan dolayı, geleneksel siber güvenlik yöntemleri ile korunmaları çok daha zordur [12].

III. BİLGİ GÜVENLİĞİ

Bilgi güvenliği, bilgi kavramının yetkisi olmayan kişiler tarafından görüntülenmesini, kullanılmasını, değiştirilmesini, silinmesini ve zarar verilmesini önleme süreçleri olarak ifade edilebilir [13]. Bilgi güvenliği kavramının tarihi, bilgisayar güvenliği ile birlikte başlamıştır. İlk uygulamalarından itibaren güvenlik, fiziksel konumları, cihazları ve yazılımları siber tehditlerden korumayı amaçlamaktadır. Bilgi güvenliği, çeşitli iş akışları ile oluşturulan veri ve bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini depolama, işleme ve iletim ortamlarının tümünde korumak için kullanılmaktadır. Bilgi güvenliğinden mümkün olan en iyi şekilde yararlanabilmek için gerekli güvenlik politikaları oluşturmak ve düzenlenecek eğitimler ile çalışanlara yeterli bilinci kazandırmak önemlidir [14].

İşletmelerde bilginin yönetimi ve güvenliğinin sağlanması konusunda en çok görev alan iki birimin çalışanları yöneticiler ve bilgi teknolojileri uzmanlarıdır. Bu iki gruptaki çalışanlar, en riskli eylemler ile sürekli karşı karşıya kalmaktadırlar. İşletmelerin en çok değer verdiği ve gizli tutmaya çalıştığı bilgileri de gören, kullanan ve kayıt altına alanlar da yine bu çalışanlardır. Ayrıca yaptıkları işlerin niteliklerinden dolayı işletme içerisinde en çok dikkat çeken ve örnek alınan kişiler yöneticiler ve bilgi teknolojileri uzmanları olarak gösterilmektedir. İşletmelerde bilgi güvenliği konusunda üst yönetim tarafından gerekli önlemler alınmaya çalışılsa da genellikle günü kurtarıcı ve teknoloji tabanlı çözümlerle uygulanmaya çalışıldığı görülmektedir [15].

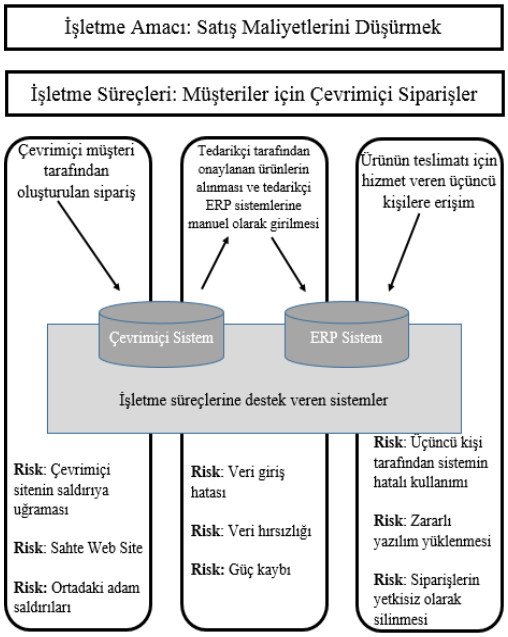
İşletmelerde, bilginin değerli bir varlık olduğu ve korunması konusunda herkesin üzerine düşen sorumlulukları anlamaları için bilgi güvenliği farkındalığının iç ve dış çevre gruplarının tamamına kazandırmak ana amaçlardan biridir. Bu durum işletmeler için son derece önem arz etmektedir. İşletme içerisindeki bilgi güvenliği politikalarının uygulanması konusunda, bilgi güvenliği çalışanlarının yanında, diğer çalışanlar, işletme paydaşları, tedarikçiler gibi işletme süreçleri ile bağlantısı olan herkes sorumludur. Bu kapsamda oluşturulacak olan farkındalık ile çalışanlarda güvenlik bilincinin oluşturulurken, korunması gereken bilgilerin hangileri oldukları, hangi tür saldırılara karşı korunmaları gerektikleri konularında yeterli bilinç kazandırılabilir. Eğer bir çalışan bilgi güvenliği konusunda sahip olacağı sorumluluğu kendi iş sorumluluğu olarak görebilirse, o zaman konu hakkında yeterli bilinç kazanmış olur. Bunun içinde gerekli eğitim çalışmalarının, yönetim kademesi tarafından planlanması gerekmektedir [16].

A. Endüstri 4.0 ve Güvenlik Endişeleri

Endüstri 4.0 devrimi ile üretim sistemindeki cihazların bilgisayar ağı altyapısı ile birbirlerine bağlanmaları ve veri alışverişinde bulunmaları amacıyla kullanılan M2M sistemleri, mevcut olan tüm güvenlik tehlikeleri ile başa çıkmak zorunda kalmıştır. M2M sistemler, internet dünyasına yeni tehditler kazandırmamıştır, ancak var olan tehditlerin etki alanının ve vereceği zararın boyutunu arttırmıştır [17]. Veri gizliliği, kimlik doğrulama, bütünlük, reddedilme ve kullanılabilirlik kavramları, güvenlik sistemleri içerisinde değerlendirilmesi gereken ana konular olarak göze çarpmaktadır. Ancak, M2M sistemler için bu güvenlik sistemlerinin kullanılması hakkında bir standart bulunmamaktadır. M2M sistemler içerisinde bulunan zeki makineler ve bilgisayarlar, internet tabanlı daimi iletişim içerisinde bulunduklarından dolayı çeşitli aktif ve pasif saldırılara karşı savunmasız durumdadır [12].

Endüstri 4.0 kapsamında da kullanılan yeni nesil M2M sistemlerinde, klasik sensor ağlarında olduğu gibi, cihazlar arasında yapılan veri alışverişinin gizliliği, bütünlüğü, kimlik denetimi ve erişim kontrolü gibi güvenlik gereksinimleri bulunmaktadır. Bu gereksinimler, sisteme şifreleme teknikleri gibi çeşitli iletişim teknolojilerini dahil ederek veya güvenlik duvarı gibi harici sistemleri kullanarak karşılanabilir. Ayrıca cihazlar arasındaki iletişimin internet tabanlı olması, sistemin güvenlik gereksinimlerine esneklik ve dayanıklılık kavramlarını da eklemektedir [18].

Teknolojik gelişmeler, işletmelerin verimliliklerini ve performanslarını arttırabilmeleri için günlük iş süreçlerinde eşi benzeri görülmemiş bir baskı oluşturmuştur. Gerçekte işletmeler, yeni teknolojilerin ortaya çıkması ile birlikte daha kolay iş süreçlerini ortaya çıkartan işletme aktivitelerini geliştirmek için bilgi ve iletişim teknolojilerinin performansına ciddi anlamda bel bağlamaktadırlar. Bulut tabanlı sistemler, nesnelerin interneti ve endüstri 4.0, teknolojik değişimler konusunda yeni girişimler başlatmış fakat bunlarla beraber yeni güvenlik risklerinde de artışa sebep olmuştur. Birbirleri ile bağlantılı olan sistemler, işletmeler için kritik dereceye ve finansal etkilere sahip birçok güvenlik riskine maruz kalma oranını önemli ölçüde arttırmaktadır. Sistemlere zarar verme amacı güden siyah şapkalı korsanlar, özellikle üretim zincirini aksatmak için sistem bileşenlerinde bulunan yazılım açıklarını kullanarak saldırı gerçekleştirmektedirler. [19].



Şekil 2. İşletme süreçlerinde karşılaşılabilecek bazı güvenlik riskleri [19]

Birbirleri ile bağlantılı olup iletişim halinde bulunan cihazların oluşturduğu ağlar, saldırılara karşı açık durumda bulunmaktadır. Bilgi ve iletişim teknolojilerinin sahip olduğu güvenlik risklerinin tamamı bu tür bağlantılı sistemler için de geçerli durumdadır. Özellikle internete bağlı sistemlerin oluşturduğu nesnelerin interneti kavramı güvenlik açısından kritik alan oluşturmaktadır [20]. İşletmelerin bağlantılı cihazlar ile oluşturulacak M2M sistemlerinin imkanlarından tam olarak faydalanabilmeleri için sistemin kuruluşunu, cihaz ve veri iletiminin sisteme nasıl dahil edileceğini anlayabilmeleri, ayrıca gizlilik endişeleri ile güvenlik problemlerinin arttığı bir kavramda bu sistemi nasıl kullanabileceklerini öğrenmeleri son derece önem arz etmektedir. Gizlilik ve güvenlik konusunda oluşan kaygıların artması, bu teknolojinin benimsenmesi sürecini geciktirme ihtimalini de yükseltmektedir [8].

Endüstri 4.0 yapısında, birbirleri ile bağlantılı olan cihazlar arasında akan veriyi illegal yollarla elde edebilmek için, zararlı yazılımlar yüklü ve yüksek kapasiteye sahip bilgisayarlar ile dahil olmak istenebilir. Bu tür bir bilgisayarı yöneten korsan, bulacağı sistem açıkları ile M2M ağına sızarak veri okumaya veya sistemi işlemez hale getirmeye çalışabilir. Bunun yanında korsan, yine sistem açıklarından faydalanarak farklı bir cihazı ağa dahil etmek yerine, ağdaki mevcut cihazlardan birini kendi kontrolü altında almaya çalışabilir ve ele geçirdiği cihaz üzerinden veri okumak veya sistemin çalışmasını engellemek isteyebilir. Karşılaşılabilecek tüm bu saldırılardan korunabilmek için gerekli bilgi güvenliği politikalarının oluşturulması ve gerekirse kriptoloji biliminden yararlanılması önem arz etmektedir [21].

IV. İLGİLİ ÇALIŞMALAR

Bağlantılı cihazlar arasında kurulan iletişim sisteminin ve gerçekleştirilen veri alışverişinin güvenliğinin sağlanması konusunda çeşitli zorluklarla karşı karşıya kalınmaktadır. Bu kapsamda, Qiu vd. çalışmalarında çok alanlı M2M sistemleri için kriptografi ve gelişmiş şifreleme standardı olan AES sistemini içeren sertifikasız hibrit bir şifreleme şeması ile çalışan anonim kimlik doğrulama sistemi geliştirmişlerdir. Yapılan testlerde, geliştirilen sistemin birçok siber saldırıya karşı başarılı olduğu sonucuna ulaşmışlardır [22].

Yeh vd. zeki cihazların güvenli iletişimi için sertifikasız bir imza şeması sunmuş ve başarılı test sonuçlarına ulaşmıştır [23]. Sonrasında yapılan bir başka çalışmada, Yeh ve arkadaşları tarafından oluşturulmuş olan şema hakkında iki adet eksik tespit ettiklerini, hatta oluşturulmuş olan şemanın genel anahtar saldırılarına karşı savunmasız olduğunu belirtmişler ve eksiklikleri giderecek yeni bir sertifikasız imza şeması önermişlerdir [24].

King tarafından yapılan çalışmada, bir mikroişlemci ile kontrol edilebilen cihazların nesnelerin interneti sistemi içerisine dahil edilebilmesi ve bu cihazlar arasında internet aracılığı ile akan verinin gizlilik ve güvenilirliğinin sağlanması amacıyla kullanılabilecek bir güvenlik şeması geliştirilmesi amaçlanmıştır. Uygulanan testlerde geliştirilen şemanın, verinin gizliliği, bütünlüğü ve güvenliğinin yeterli ölçüde sağlandığı belirtilmiştir [25]. Bunun yanında Akkuş tarafından yapılan bir araştırma da, King'in çalışmasını örnek alarak nesnelerin internetinde kullanılan cihazlar arasında akan verinin WEP protokolü ile şifrelenmesi amaçlanmış. Bu yöntem ile de veri gizliliği sağlandığı ortaya konmuştur [26].

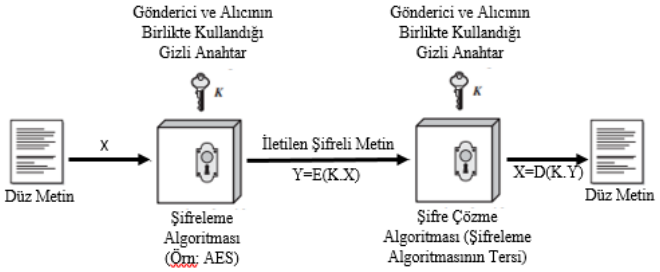
Bağlantılı cihazlar arasında gerçekleştirilen veri alışverişinin güvenliğinin sağlanması konusunda özellikle sağlık sektörü ile ilgili çalışmalar da yapılmıştır. Moosavi vd. sensörler ile donatılmış sağlık uygulamalarına ait cihazlar ile hastalar ve doktorlar arasında internet aracılığı ile daimi bir iletişim kurmayı ve bu iletişimin kimlik doğrulama ve yetkilendirme özellikleri ile güvenli bir şekilde gerçekleştirilmeyi amaçlamıştır [27]. Yine sağlık uygulamalarında kullanılan ve nesnelerin internetine dahil olan sağlık sistemleri arasında veri gizliliği ve güvenliğinin sağlanması için bir anahtar yönetim protokolü önerilmiştir [28]. Ayrıca Can vd. çalışmalarında, sağlık uygulamaları üzerine yapılan diğer çalışmalar gibi hasta mahremiyetinin en yüksek seviyede sağlanabilmesi amacıyla verinin gizliliği ve güvenliğini amaçlayan anlamsal web teknolojileri ile desteklenmiş bir sistem önerisinde bulunmuşlardır [29].

V. SİSTEM ÖNERİSİ

Siber fiziksel sistemler içerisinde kullanımda bulunan M2M sistemler arasında akan bilginin güvenliğinin ve gizliliğinin sağlanabilmesi amacıyla önerilen yapı için asimetrik ve simetrik şifreleme sistemleri incelenmiştir. İncelemeler sonucunda her iki sistemin de birbirlerine destek vereceği bir yapı oluşturulmaya çalışılmıştır.

A. Simetrik Şifreleme

Simetrik şifreleme sistemlerinde hem verinin şifrelenmesinde hem de şifrenin çözülmesi işleminde aynı gizli anahtar kullanılmaktadır. Bu sebeple daha az matematiksel işlem uygulanarak şifreleme ve şifre çözme süreçleri gerçekleşebilmektedir. Simetrik şifreleme sistemlerinin sahip olduğu bu özellik, hızlı ve güvenli bir şifreleme sistemi oluşturulmasına imkan sağlamaktadır. Ancak burada anahtar dağıtım problemi ortaya çıkmaktadır. Şifreleme anahtarının gönderici ve alıcı arasında güvenli bir şekilde iletiminin yapılmış olması gerekmektedir [30]. Şekil 3'te simetrik şifreleme algoritmalarının basitleştirilmiş bir modeli görülmektedir.

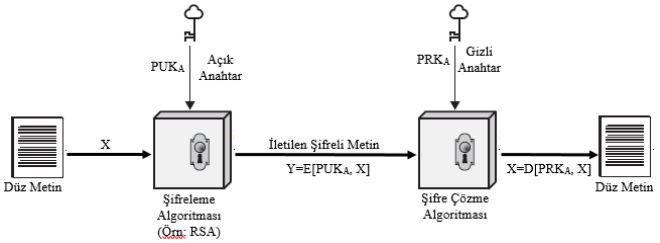


Şekil 3. Basitleştirilmiş Simetrik Şifreleme Modeli [31]

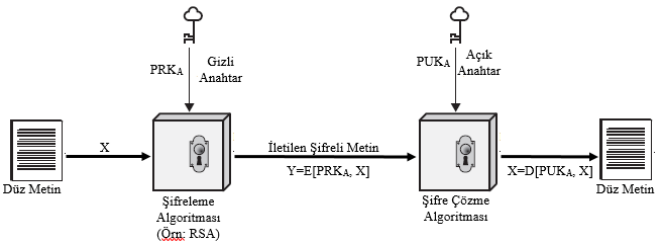
Simetrik şifreleme sistemlerinin güvenli bir şekilde kullanılabilmeleri için sahip olmaları gereken iki şart bulunmaktadır. Birincisi güçlü bir şifreleme algoritmasıdır. Kullanılacak olan algoritma şifreleme işlemi sonucundan elde edilen şifreli metnin, gizli anahtar olmadan şifresini çözülmesini özellikle kaba kuvvet saldırılarına karşı engelleyebilmelidir. İkinci şart, gönderici ve alıcı gizli anahtarın kopyalarını güvenli bir şekilde elde etmeleri gerekmektedir. Ayrıca sonraki süreçte de anahtarın gizliliğini sağlamaya devam etmeliler. Eğer anahtar bir başkasının eline geçerse, tüm iletişim okunabilir olacaktır. Simetrik şifreleme sistemlerinde güvenli iletişim için asıl olan algoritmanın değil, anahtarın gizliliğinin sağlanmasıdır. Kullanılan algoritmanın bilinmesi sebebiyle verinin şifresinin çözülmesi işlemi pratik bir yöntem değildir. Bu sebeple ne olursa olsun algoritmanın değil, anahtarın gizli kalması son derece önemlidir [32].

B. *Asimetrik Şifreleme*

Asimetrik şifreleme algoritmaları, simetrik şifreleme algoritmalarına göre önemli bir farklılık göstermektedir. Bu da şifreleme ve şifre çözme işlemleri için birbirinden farklı anahtarların kullanılması durumudur. Asimetrik şifreleme sistemlerini kullanan her kişide açık ve gizli olarak adlandırılan bir anahtar çifti bulunması gerekmektedir. Algoritmada kullanılan açık anahtar, herkese rahatlıkla dağıtılabilecek olan gizli tutulmasına gerek bulunmayan bir anahtar türüdür. Gizli anahtar ise, sahip olunan kişi tarafından gizli tutulması gereken anahtar türüdür. Bu sistem ile şifreleme yapacak olan kişi hedef kişinin açık anahtarını kullanarak veriyi şifreler ve hedefe gönderir. Kaynak tarafından şifrelenmiş olan veri, sadece hedef kişinin sahip olduğu gizli anahtar ile çözümlenebilir. Ayrıca kaynak olan kişi, veriyi göndermeden önce kendi gizli anahtarı ile şifreleyerek imzalayabilir ve hedef kişi, kaynak kişinin açık anahtarını kullanarak imzayı doğrulayabilir. Asimetrik şifreleme algoritmaları, kullanılan anahtarlarından birinin halka açık olmasından dolayı birçok kaynakta açık anahtarlı şifreleme olarak da adlandırılmaktadır [30]. Şekil 4a ve 4b'de asimetrik şifreleme modellerinin çalışma mantığı gösterilmektedir.



a) Açık Anahtar ile Şifreleme



b) Gizli Anahtar ile Şifreleme

Şekil 4. Basitleştirilmiş Asimetrik Şifreleme Modelleri [31].

C. *Hibrit Şifreleme Şeması*

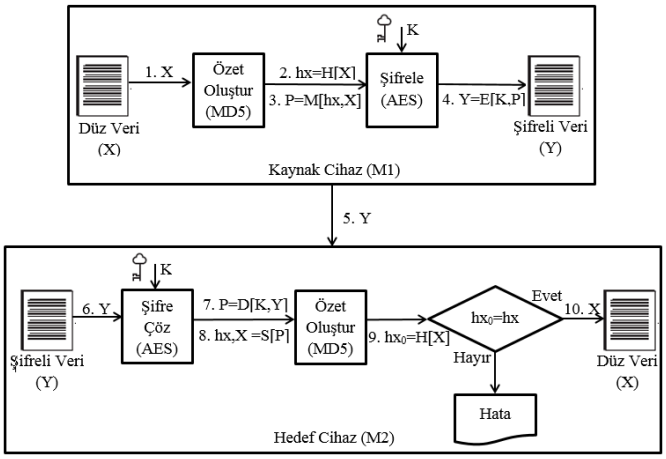
Endüstri 4.0 teknolojisinde kullanılan M2M sistemlerinde akan verinin gizliliğinin ve güvenliğinin sağlanabilmesi amacıyla önerilen sistem, verinin kaynak ve hedef makineler arasında şifrelenerek gitmesini kapsamaktadır. Bu yapı içerisinde kullanılmak üzere, hız ve performans açısından daha yüksek özelliklere sahip olduğundan dolayı simetrik şifreleme algoritmalarından AES algoritmasının kullanımı tavsiye edilmektedir.

AES algoritması, bir blok şifreleme algoritmasıdır. 128 bit boyutundaki veri bloklarını 128,196 veya 256 bitlik anahtar ile şifrelemektedir. Algoritmada kullanılan anahtarın boyutu, şifreleme ve şifre çözme süreçlerinin kaç tur tekrarlanacağını belirlemektedir (128 bit anahtar 10 tur, 196 bit anahtar 12 tur ve 256 bit anahtar 14 tur) [33].

Önerilen şema doğrultusunda, cihazlar arası yapılacak güvenli veri alışverişinin işlemleri Şekil 5'te ayrıntılı bir biçimde gösterilmektedir.

Tablo 1. Şifreli Veri İletim Şeması Sembollerinin Tanımları

Sembol	Tanım
X	Şifrelenmemiş düz veri
Y	Şifrelenmiş veri
hx	M1 tarafından oluşturulan "X" veri özeti
hx_0	M2 tarafından oluşturulan "X" veri özeti
P	Verinin kendisi ve özetinin bulunduğu veri paketi
K	Simetrik şifreleme anahtarı
H	Özet oluşturma işlemi
E	Şifreleme İşlemi
D	Şifre çözme işlemi
M	Veri ile veri özetini birleştirme işlemi
S	Veri ile veri özetini ayrıştırma işlemi
MD5	Özet oluşturma algoritması
AES	Simetrik şifreleme algoritması



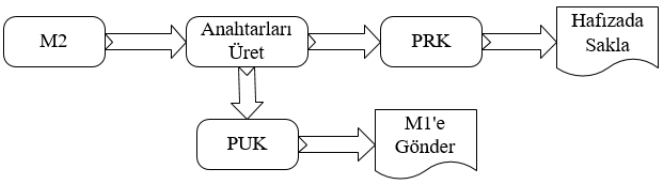
Şekil 5. M2M Sistemde AES Algoritması ile Şifreli Veri İletimi

1. **X:** Bu sembol, makineler arasında transferi yapılacak olan veriyi ifade etmektedir. M1 tarafından oluşturulan X verisi, şifrelenmemiş düz veri formundadır.
2. **hx = H[X]:** M1 tarafından X verisi oluşturulduktan sonra veri bütünlüğü kontrolü ve verinin kimliklendirilmesi amacıyla özeti oluşturulur. Bu yapı içerisinde, veri özetinin oluşturulması için MD5 algoritması tercih edilmiştir.
3. **P = M[hx,H]:** Oluşturulan özetin verinin kendisine eklenmesi sureti ile P veri paketi elde edilmektedir. P veri paketi, şifrelenerek M2'ye gönderilecek olan pakettir.
4. **Y = E[K,P]:** M2 makinesine gönderilmek üzere hazırlanan P veri paketi, 256 bitlik simetrik K anahtarı ile AES algoritmasına bağlı olarak şifrelenmektedir. Bu işlem sonucunda, şifreli veriden oluşan Y veri paketi elde edilmektedir.
5. **Y:** M1 tarafından gerçekleştirilen süreçler sonucunda üretilen şifreli Y veri paketi M2 makinesine, bilgisayar ağı alt yapısı kullanılarak gönderilmektedir.
6. **Y:** Bu aşamada kullanılan Y sembolü, M1 makinesi tarafından gönderilmiş olan şifreli veri paketini temsil etmektedir. M2, bu şifreli veri paketinde şifre çözme işlemleri uygulayarak orijinal veriye ulaşmaya çalışacaktır.
7. **P = D[K,Y]:** M2, gelen şifreli veri paketine, aynı 256 bitlik simetrik K anahtarını kullanarak şifre çözme işlemi uygulamaktadır. Bu süreç sonunda M2, kendisine M1 tarafından gönderilmiş olan P veri paketine ulaşmaktadır.
8. **hx,X = S[P]:** P veri paketi elde edildikten sonra, ayrıştırma işlemi yapılarak, X verisi ve hx veri özeti ortaya çıkartılmaktadır. Gelen X verisi, M2 makinesine gönderilmek üzere, M1 tarafından üretilmiş olan şifresiz düz veri formudur. hx ise, M1 tarafından oluşturulmuş olan X verisinin özet bilgisidir.
9. **hx_0 = H[X]:** Bu adımda, M2 tarafından da X verisine ait bir özet oluşturulmaktadır. Amaç, M1 tarafından veri paketi içerisinde gönderilmiş olan hx özet bilgisi ile M2 tarafından oluşturulan hx_0 özet bilgisini karşılaştırmaktır. Bu karşılaştırma sonucunda, her iki özet bilgisi birbirinin aynısı olursa veri bütünlüğü sağlanmış olur. Eğer karşılaştırma sonucu eşitlik sağlanamazsa, veri bozulmuş veya sisteme dışarıdan sızmaya çalışan üçüncü bir cihaz tarafından üretilmiş olduğu şeklinde yorumlanabilir.
10. **X:** Son sürece gelindiğinde, M1 makinesi tarafından üretilmiş olan X verisi gizliliği ve güvenliği sağlanarak M2 makinesine ulaşmış olacaktır. Süreç, yeni verilerin üretilmesi ve transfer edilmesi şeklinde devam edecektir.

M2M sistem içerisinde veri şifreleme ve şifre çözme süreçlerinde simetrik şifreleme algoritmalarının kullanımı, veri iletiminin hızlı ve verimli olmasını sağlarken, anahtar paylaşımı sorununu da ortaya çıkartmaktadır. Çünkü gönderici ve alıcı aynı anahtarı kullanmakta, bundan dolayı üretilen anahtarın iki tarafta da bulunması gerekmektedir. Yani anahtarın güvenli bir kanal oluşturularak hem göndericiye hem de alıcıya ulaştırılması sağlanmalıdır. Bu işlem için kullanılabilecek en güvenli yöntemlerden biri üretilmiş olan simetrik şifreleme anahtarının, asimetrik şifreleme algoritmalarından biri ile şifrelenerek muhataplarına iletilmesidir. Bu konuda RSA algoritması kullanılabilir.

RSA algoritması, çok büyük değerdeki asal sayıların üzerine yapılacak hesaplamalardaki yüksek seviyeli zorluktan yararlanılarak oluşturulmuştur. RSA algoritması kullanılarak gerçekleştirilen şifreleme işlemleri başlıca kullanım alanları arasında anahtar iletimi için küçük miktarlarda verilerin şifrelenmesi ve internette dijital sertifikalar için elektronik imzaların oluşturulması belirtilmektedir. Bunların dışında çok daha farklı amaçlar için uygulanacak şifrelemelerde RSA algoritması kullanılabilmektedir [34]. RSA algoritmasının gücü, rastgele belirlenen çok büyük değerdeki asal sayılar ile elde edilen n sayısının modüler çarpanlarına ayrılmasındaki zorluğa dayanmaktadır. [35].

M2M sistem içerisinde kullanılacak AES simetrik şifreleme anahtarının makineler arasında iletilmesinde asimetrik şifreleme algoritması olan RSA sisteminin kullanılabilmesi için makinelerin biri tarafından (Örn: M2) açık anahtar (PUK) ve gizli anahtarın (PRK) oluşturulması ve açık anahtarın diğer makineye (Örn: M1) iletilmesi gerekmektedir (Şekil 6).

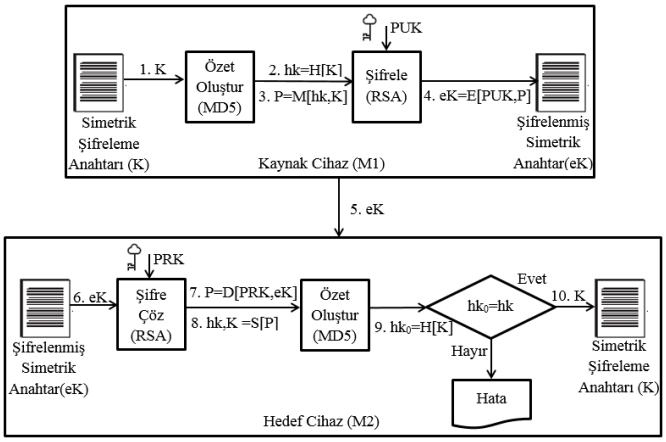


Şekil 6. Açık ve Gizli Anahtarın Üretilmesi ve Açık Anahtarın Alıcıya İletilmesi

Asimetrik şifreleme anahtarlarının üretilmesi ve açık anahtarın iletilmesinden sonra sıra M1 tarafından oluşturulacak olan AES şifreleme anahtarının M2 makinesine iletilmesi gerekmektedir (Şekil 7).

Tablo 2. Anahtar Paylaşımı Şeması Sembollerinin Tanımları

Sembol	Tanım
K	AES Simetrik Şifreleme Anahtarı
eK	Şifrelenmiş Simetrik Anahtar
hk	M1 tarafından oluşturulan “K” veri özeti
hk_0	M2 tarafından oluşturulan “K” veri özeti
P	Verinin kendisi ve özetinin bulunduğu veri paketi
PUK	Asimetrik Şifreleme için Açık Anahtar
PRK	Asimetrik Şifre Çözme için Gizli Anahtar
H	Özet oluşturma işlemi
E	Şifreleme İşlemi
D	Şifre çözme işlemi
M	Veri ile veri özetini birleştirme işlemi
S	Veri ile veri özetini ayrıştırma işlemi
MD5	Özet oluşturma algoritması
RSA	Asimetrik şifreleme algoritması

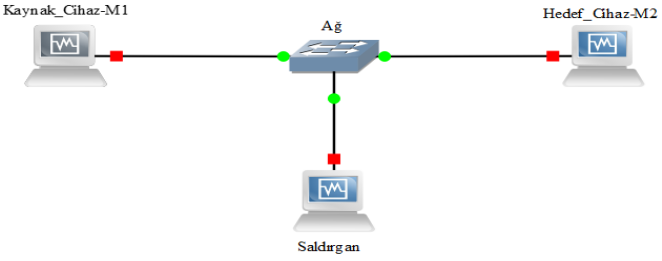


Şekil 7. AES Şifreleme Anahtarının Üretilmesi ve Asimetrik Şifreleme Tekniği ile Makineler Arasında Paylaşılması

1. **K:** Bu sembol, makineler arasında güvenli veri aktarımı yapılabilmesi için üretilen 256 bitlik AES simetrik şifreleme anahtarını temsil etmektedir. Şemaya göre K anahtarı, M1 tarafından üretildikten sonra asimetrik şifreleme (RSA) algoritmasına göre şifrelenerek M2 makinesine güvenli bir şekilde iletilecektir.
2. **hk = H[K]:** K anahtarının iletimine başlanmadan önce kimliklendirme ve bütünlük amaçlarının gerçekleştirilebilmesi için veri özeti oluşturulmaktadır. K anahtarının veri özetinin oluşturulmasında, veri akış şemasında olduğu gibi MD5 özet algoritmasından faydalanılmaktadır.
3. **P = M[hk, K]:** Oluşturulan anahtar özetinin, K anahtarına eklenmesi sonucundan P veri paketi elde edilmektedir. Şifrelenmeden önceki bu adım, açık anahtar ile koruma altına alınacak veriyi ifade etmektedir.
4. **eK = E[PUK, P]:** M2 makinesine gönderilmek amacıyla hazırlanan P verisi, M2’ye ait olan açık anahtar PUK ile şifrelenerek eK şifrelenmiş anahtar verisi elde edilmektedir. Asimetrik şifrelemenin doğası gereği açık anahtarın herkes tarafından kullanımı serbesttir. Ancak, şifrelenen eK verisinin çözümlenebilmesi için sadece M2 tarafından kullanılabilecek olan gizli anahtar kullanılmasının zorunlu olması, veri alışverişlerinde kullanılacak olan K simetrik anahtarının güvenli bir şekilde paylaşılmasını sağlamaktadır.
5. **eK:** Şifrelenmiş olan veri artık güvenli bir şekilde hedef makineye (M2) gönderilmektedir. Eğer bu aşamada veri yetkisiz kişilerin eline geçerse, onlar için anlamsız olacaktır.
6. **eK:** M2, kendisine gönderilen şifreli veriyi çözümlemek için gerekli süreçleri bu aşamada başlatmaktadır.
7. **P = D[PRK, eK]:** M2’nin şifreli veri paketini aldıktan sonra uygulayacağı ilk süreç, şifrenin çözülmesini sağlamaktır. Şifrenin çözülmesi ile M1 tarafından oluşturulmuş olan ve içerisinde hem K anahtarını hem de anahtar özet bilgisini bulunduran P veri paketini elde etmektedir.
8. **hk, K = S[P]:** M2, P veri paketi üzerinde uygulanan ayrıştırma işlemi ile anahtar özeti olan hk ve simetrik şifreleme anahtarı olan K değerlerine ulaşmaktadır. K anahtarı, makinelerin olağan süreçlerinde birbirleri arasında güvenli veri aktarımı yapabilmeleri için kullanılacaktır. hk anahtar özeti ise anahtarın bütünlüğünü kaybetmeden hedefe ulaşıp ulaşmadığının kontrol edilmesinde kullanılmaktadır.
9. **hk_0 = H[K]:** M2, kendisine ulaşan K anahtarının özeti çıkartmaktadır. Bu süreçteki amaç, M1 makinesinden K anahtarı ile birlikte gelen hk özetinin, kendi oluşturacağı özet hk_0 ile aynı olup olmayacağının tespit edilmesidir. Eğer hk ve hk_0 özetleri birbirilerine eşit olmazlarsa, veri aktarımında problemler olduğu ve gelen K anahtarının veri alışverişlerinde kullanılamayacağı anlamına gelir. Bu tür bir durumla karşılaşıldığında tüm süreçler durdurularak, güvenlik testlerinin yapılması ve işlemlerin baştan başlayarak tekrar edilmesi gerekmektedir. Özetler birbirine eşit çıkarsa, veri bütünlüğünün zarar görmediği ve K anahtarının M1 üzerinde üretildiği şekli ile M2’ye ulaştığı veri aktarımında güvenle kullanılabileceği anlamına gelir.
10. **K:** Simetrik şifreleme anahtarı K, gizliliği ve güvenliği sağlanarak iki cihaz arasında paylaşılmıştır. Bu aşamadan sonra makineler, güvenli veri aktarımına başlayabilirler.

VI. DENEYSEL ÇALIŞMA

Çalışma kapsamında önerilen şemanın test edilebilmesi için GNS3 v2.1.11 yazılımı ile bilgisayar ağı simülasyonu oluşturulmuştur.

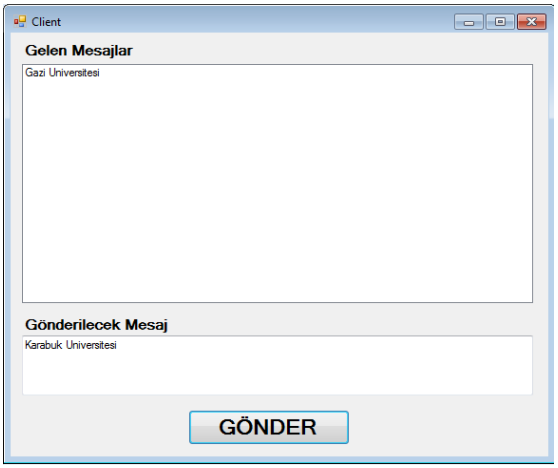


Şekil 8. Bilgisayar Ağı Simülasyonu

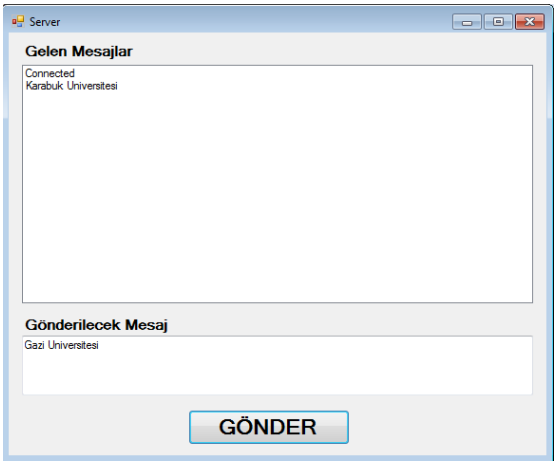
Simülasyon içerisinde, birbirleri arasında veri transferi yapacak olan iki adet Windows 7 işletim sistemi yüklü sanal cihazlar, akan veriye saldırı düzenleyebilmek için de Kali Linux işletim sistemi yüklü bir adet sanal cihaz kurulmuştur. Sanal cihazların tamamı 1 GB kapasiteli RAM belleğe ve 16 MB kapasiteli ekran belleğine sahip olacak şekilde Oracle VM VirtualBox uygulaması üzerinden simülasyonda çalıştırılmıştır.

Veri transferi yapacak olan cihazlar arasındaki aktarımın yönetilebilmesi amacıyla C# Programlama Dili ile herhangi bir güvenlik şeması bulunmayan ve çalışma içerisinde önerilmiş olan güvenlik şemasını kullanan iki farklı iletişim yazılımı oluşturulmuştur. Kali Linux işletim sistemi yüklü olan cihaz içerisinde mevcut olan Ettercap isimli yazılım aracılığı ile diğer iki cihaz arasında gerçekleşen veri akışına ARP Zehirleme (ARP Poisonning) saldırısı uygulanmıştır.

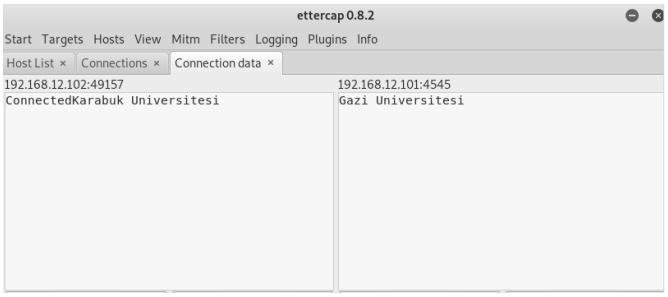
İlk testte, herhangi bir güvenlik şeması kullanılmayan yazılımlar ile cihazlar arasında veri akışı sağlanmış ve bu akışa atak yapılmıştır. İşlem sonucunda, normal şartlarda sadece iki cihaz arasında kalması gereken verinin sürece illegal yollar ile dahil olan üçüncü bir cihaz tarafından net bir şekilde elde edilebildiği görülmüştür. Ayrıca testin bu aşaması ile kullanılan saldırı türünün tehlikesi gösterilmiştir (Şekil 9).



a) Kaynak Cihaz (M1) Veri Aktarımı



b) Hedef Cihaz (M2) Veri Aktarımı

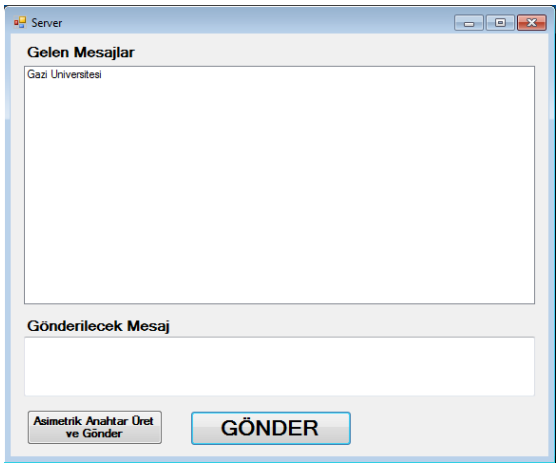


c) Saldırı Sonucu

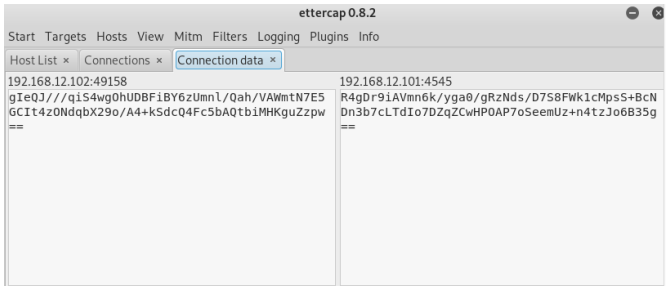
Şekil 9. Güvenlik Şeması kullanılmayan Veri İletimine Yapılan Siber Atak

Testin ikinci aşamasında ise hibrit güvenlik şeması kullanılarak cihazlar arasında veri aktarımı gerçekleştirilmiştir. Bu iletişime yapılan saldırı sonucunda cihazlar arasında akan veri sadece şifrelenmiş bir şekilde ele geçirilmiştir. Sonuç olarak veri, atak yapan bilgisayar tarafından tamamen okunamaz halde görüntülenebilmektedir (Şekil 10).

a) Kaynak Cihaz (M1) Veri Aktarımı



b) Hedef Cihaz (M2) Veri Aktarımı



c) Saldırı Sonucu

Şekil 10. Önerilen Güvenlik Şemasını Kullanılarak Gerçekleştirilen Veri İletimine Yapılan Siber Atak

Sonuç olarak önerilen hibrit güvenlik şeması tarafından, cihazlar arasında gerçekleştirilen veri iletiminin güvenliğinin sağlandığı görülmüştür.

VII. TARTIŞMA VE SONUÇ

Endüstri 4.0 teknolojilerinde kullanılan M2M sistemler içerisinde veri gizliliği ve güvenliğinin sağlanması amacıyla önerilen hibrit sistem ile işletmelerin üretim sistemleri içerisinde oluşturdukları iletişim yapısının yetkisiz kişi veya kurumlar tarafından öğrenilmesini engellemeleri amaçlanmaktadır. Hibrit şema ile makineler asimetrik şifreleme algoritmalara göre daha hızlı ve performanslı şifreli iletişim imkanı sunan simetrik şifreleme algoritmalarını kullanılması tavsiye edilmektedir. Ancak simetrik şifreleme algoritmalarında ortaya çıkan anahtar paylaşım sürecinin gizlilik ve güvenliğinin sağlanabilmesi için de asimetrik sistemlerin kullanılması gündeme gelmektedir. Ayrıca gerçekleştirilecek olan veri iletişiminde özet bilgisi oluşturma algoritmaları ile kimlik doğrulama yapısı oluşturulabilir ve veri bütünlüğü de kontrol edilebilir duruma getirilebilir.

Önerilen bu yapı, M2M sistemlerin haricinde nesnelerin interneti teknolojisi ile kişisel kullanımlarda dahi kullanılabilir durumdadır. Bu amaçla kişiler, kendi kişisel bilgilerin aktarımlarının gerçekleştirdiği cihazlar arasında akan verinin gizlilik, güvenlik ve bütünlüğünü kontrol altına alabilirler.

İleriki süreçlerde, önerilen yapının endüstri simülasyonları ve prototip üretim sistemleri üzerinde uygulanması planlanmaktadır. Yapılacak olan devam çalışmasında hibrit şifreleme sisteminin güvenilirliği ve performansının test edilmesi ve üretim verimliliğine etkisinin araştırılması süreçleri uygulanacaktır.

KAYNAKÇA

[1] E. Sayılgan ve Y. İşler, «Medikal Endüstri 4.0 ile TÖbbi Cihaz Sektörü,» %1 içinde *Tıp Teknolojileri Kongresi*, Trabzon, 2017.

[2] İ. Akben ve İ. İ. Avşar, «Endüstri 4.0 ve Karanlık Üretim: Genel Bir Bakış,» *Türk Sosyal Bilimler Araştırmaları Dergisi,* cilt 3, no. 1, pp. 26-37, 2018.

[3] H. Kagermann, W. D. Lukas ve W. Wahister, «Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution,» *Vdi Nachrichten*, p. 2, 2011.

[4] S. Alçın, «Üretim İçin Yeni Bir İzlek: Sanayi 4.0,» *Journal of Life Economics,* no. 8, pp. 19-30, 2016.

[5] S. Heng, «Industry 4.0 Upgrading of Germany's Industrial Capabilities on the Horizon,» *Deutsche Bank Research,* pp. 1-16, 23 04 2014.

[6] S. Weyer, M. Schmitt, M. Ohmer ve D. Gorecky, «Towards Industry 4.0 - Standardization As the Crucial Challenge For Highly Modular, Multi-Vendor Production Systems,» *IFAC-PapersOnLine*, cilt 48, no. 3, pp. 579-584, 2015.

[7] P. K. Verma, R. Verma, A. Prakash, A. Agrawal, K. Naik, R. Tripathi, M. Alsabaan, T. Khalifa, T. Abdelkader ve A. Abogharaf, «Machine-to-Machine (M2M) Communications: A Survey,» *Journal ofNetworkandComputerApplications,* no. 66, pp. 83-105, 2016.

[8] S. Greengard, Nesnelerin İnterneti, İstanbul: Optimist Yayın, 2017.

[9] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld ve M. Hoffmann, «Industry 4.0,» *Business & Information Systems Engineering,* cilt 6, no. 4, pp. 239-242, 2014.

[10] H. Polat ve S. Oyucu, «Token-based authentication method for M2M platforms,» *Turkish Journal of Electrical Engineering & Computer Sciences,* no. 25, pp. 2956-2967, 2017.

[11] J. Shen, T. Zhou, X. Liu ve Y.-C. Cheng, «A Novel Latin-Square-Based Secret Sharing for M2M Communications,» *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS,* cilt 14, no. 8, pp. 3659-3668, 2018.

[12] H.-C. Chen, I. You, C.-E. Weng, C.-H. Cheng ve Y.-F. Huang, «A Security Gateway Application for End-to-End M2M Communications,» *Computer Standards & Interfaces,* no. 44, pp. 85-93, 2016.

[13] Ş. Şen ve T. Yerlikaya, «ISO 27001 Kurumsal Bilgi Güvenliği Standardı,» %1 içinde *Akademik Bilişim 2013*, Antalya, 2013.

[14] M. E. Whitman ve H. J. Mattord, Principles of Information Security Fourth Edition, Boston, USA: Course Technology, Cengage Learning, 2012.

[15] M. Eminağaoğlu ve Y. Gökşen, «BİLGİ GÜVENLİĞİ NEDİR, NE DEĞİLDİR, TÜRKİYE' DE BİLGİ GÜVENLİĞİ SORUNLARI VE ÇÖZÜM ÖNERİLERİ,» *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* cilt 11, no. 4, pp. 1-15, 2009.

[16] E. Şahinaslan, A. Kantürk, Ö. Şahinaslan ve E. Borandağ, «Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluişturma Yöntemleri,» *XI. Akademik Bilişim Konferansı*, Şanlıurfa, 2009.

[17] A. Barki, A. Bouabdallah, S. Gharout ve J. Traoré, «M2M Security: Challenges and Solutions,» *IEEE Communications Survey & Tutorials,* cilt 12, no. 2, pp. 1241-1254, 2016.

[18] G. Tuna, D. G. Kogias, V. Ç. Güngör, C. Gezer, E. Taşkın ve E. Ayday, «A Survey on Information Security Threats and Solutions for Machine to Machine (M2M) Communications,» *J. Parallel Distrib. Comput.,* no. 109, pp. 142-154, 2017.

[19] T. Pereira, L. Barreto ve A. Amaral, «Network and Information Security Challenges within Industry 4.0 Paradigm,» *Procedia Manufacturing,* no. 13, pp. 1253-1260, 2017.

[20] S. F. Oktuğ ve S. B. Örs Yalçın, «Nesnelerin İnterneti Güvenliği: Servis Engelleme Saldırıları,» %1 içinde *23. Sinyal İşleme ve İletişim Uygulamaları Kurultayı*, Malatya, 2015.

[21] Y. Fu, Z. Yan, J. Cao, O. Koné ve X. Cao, «An Automata Based Intrusion Detection Method for Internet of Things,» *Mobile Information Systems,* no. 2017, pp. 1-13, 2017.

[22] Y. Qiu, M. Ma ve S. Chen, «An Anonymous Authentication Scheme For Multi-Domain Machine-toMachie Communiction in Cybere-Physical Systems,» *Computer Networks,* no. 129, pp. 306-318, 2017.

[23] K.-H. Yeh, C. Su, K.-K. R. Choo ve W. Chiu, «A Novel Certificateless Signature Scheme for Smart Objects in the Internet-of-Things,» *Sensors,* cilt 17, no. 5, p. 1001, 2017.

[24] X. Jia, D. He, Q. Liu ve K.-K. R. Choo, «An Efficient Provably-Secure Certificateless Signature Scheme for Internet of Things Deployment,» *Ad Hoc Networks,* no. 71, pp. 78-87, 2018.

[25] J. King, *A Distributed Security Scheme to Secure Data Communication between Class-0 IoT Devices and the Internet (Yüksek Lisans Tezi),* Sweden, 2015.

[26] S. Akkuş, «Nesnelerin İnterneti Teknolojisinde Güvenli Veri İletişimi: Programlanabilir Fiziksel Platformlar Arasında WEP Algoritması ile Kriptolu Veri Haberleşmesi Uygulaması,» *Marmara Fen Bilimleri Dergisi*, cilt 2016, no. 3, pp. 100-111, 2016.

[27] S. R. Moosavi, T. N. Gia, A. M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho ve H. Tenhunen, «A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways,» *Procedia Computer Science,* no. 52, pp. 452-459, 2015.

[28] M. R. Abdmeziem ve D. Tandjaoui, «An end-to-end secure key management protocol for e-health applications,» *Computers & Electrical Engineering,* no. 44, pp. 184-197, 2015.

[29] Ö. Can, E. Sezer, O. Bursa ve M. O. Ünalır, «Nesnelerin İnterneti ve Güvenli Bir Sağlık Modeli Önerisi,» %1 içinde *4th International Symposium on Innovative Technologies in Engineering and Scienc,* Antalya, 2016.

[30] H. Kodaz ve F. M. Botsalı, «Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması,» *Selçuk - Teknik Dergisi,* cilt 9, no. 1, pp. 10-23, 2010.

[31] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th Ed., Harlow, United Kingdom: Pearson Education Limited, 2016a.

[32] W. Stallings, Network Security Essentials: Applications and Standards 6. Ed, Harlow, United Kingdom: Pearson Education Limited, 2016b.

[33] M. T. Sakallı, E. Buluş, A. Şahin, F. Büyüksaraçoğlu ve N. Buluş, «AES S Kutusuna Benzer S Kutuları Üreten Simulatör,» %1 içinde *Akademik Bilişim 2006*, Denizli, 2006.

[34] M. Eriş ve M. Kaya, «CRYPTOLOCKER SALDIRILARININ İNCELENMESİ,» *İleri Teknoloji Bilimleri Dergisi,* cilt 5, no. 2, pp. 112-119, 2016.

[35] K. Shehata, H. Hussien ve S. Yehia, «FPGA Implementation of RSA Encryption Algorithm for E-Passport Application,» *International Journal of Computer and Information Engineering,* cilt 8, no. 1, pp. 82-85, 2014.