Nesnelerin İnternetinde Kriptografik Algoritmaların Performans Karşılaştırılması

Performance Comparison of Cryptographic Algorithms in Internet of Things

Berat YILMAZ
Savunma Sistem Teknolojileri Sektör Başkanlığı
Aselsan A.Ş.
Ankara, Türkiye
beyilmaz@aselsan.com.tr

Suat ÖZDEMİR
Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü
Gazi Üniversitesi
Ankara, Türkiye
suatozdemir@gazi.edu.tr

***Özetçe*— Nesnelerin İnterneti (IoT) günümüzde oldukça popüler bir kavram olup, insanların gündelik hayatında gün geçtikçe yaygınlaşan son tüketici ürünleri ile birlikte fazlasıyla tecrübe edilebilen bir alan haline gelmiştir. Dolayısıyla, bu derece yaygınlaşan bir kavram olan IoT'nin güvenliği de ayrı bir araştırma alanı oluşturmuştur. IoT cihazlarının büyük çoğunluğu fiyat-performans optimize edilecek şekilde üretilmektedir. Bu da mevcut donanımlarının uygun fiyatlı olabilmesi amacıyla kısıtlanmasıyla sonuçlanmaktadır. Bu kısıtlama kullanım alanlarına da bağlı olmakla beraber birçok güvenlik riskini de beraberinde getirmektedir. Sahip oldukları bu güvenlik risklerinin incelenmesi de birçok araştırmanın konusu olmaktadır. Bu makaleye konu olan araştırma, bu alanda yapılan bir uygulamayı ve sonuçlarını içermektedir. Farklı boyutlarda, farklı özellik ve fiyatlara sahip iki adet IoT cihazı üzerinde aynı kriptografik algoritmalar koşturulmuş, önceden belirlenen metrikler üzerinden yapılan ölçüm ve analizler ile karşılaştırmalı sonuçlar elde edilmiştir. Araştırmanın son kısmında ise elde edilen sonuçlar yorumlanmış ve araştırma tamamlanmıştır.**

Anahtar Kelimeler — nesnelerin interneti; güvenlik; kriptografik algoritmaların karşılaştırılması; enerji tüketimi karşılaştırması.

***Abstract*— Recently, Internet of Things (IoT) is a very popular concept. It has become an area that can be highly experienced with the end-user products which are becoming more and more widespread in our daily lives. Therefore, the security of IoT devices has merged as an area of the research due to its increasing usage of these devices. Most of the IoT devices are designed by considering optimum price-performance ratio. Hence, the hardware of IoT devices are constrained in order to design affordable devices. However, these constraints of IoT devices may result in a severe security risks. Hence, the examination of these security risks is a contemporary research area. In this paper, the IoT device implementation of major cryptographic algorithms is examined. The same cryptographic algorithms are run on two different IoT devices which have different constraints, different features and different prices. Tests with respect to pre-defined metrics are conducted and the measurements are analyzed by comparing the results. At the end of the paper, all results and analyzes are interpreted.**

978-1-5386-1501-0/18/$31.00 © 2018 IEEE

Keywords — internet of things; security; comparison of cryptographic algorithms; comparison of energy consumption.

I. GİRİŞ

Nesnelerin İnterneti cihazları, düşük enerji tüketimleri ve kısıtlı donanımları ile son kullanıcı pazarında üstlendikleri birçok görevi başarıyla yerine getirebilmektedirler. Cihazların donanımları, kullanım alanları ve ihtiyaçlara göre şekillenmektedir. Farklı seviyede donanımlar barındıran bu IoT cihazlarının kriptografik algoritmaları işletirken göstermiş oldukları enerji tüketim performansı bu makalenin temel araştırma konusunu oluşturmaktadır. Araştırmanın sonuçları taşınabilir, güç kaynağı olarak batarya kullanan IoT cihazları için özellikle önem taşımaktadır. Böylece bahsi geçen güvenlik alanında yoğun olarak çalıştırıldığında en optimum çalışma süresini sunan IoT cihaz ya da cihazlarının seçebilmesi problemine çözüm bulunmuş olur.

Araştırmayı gerçekleştirmek için Raspberry Pi Vakfının [1] geliştirmiş olduğu iki farklı model IoT cihazı tercih edilmiştir. Bu cihazlar sırasıyla Pi 3 Model B ve Pi Zero W modelleridir. Pi 3 yüksek enerji tüketimli yüksek performanslı IoT cihazlarını temsil etmesi amacıyla seçilmişken; Pi Zero düşük enerji tüketimli düşük performanslı IoT cihazlarını temsil etmesi amacıyla seçilmiştir.

Araştırma kapsamında, bu cihazlar üzerinde, çeşitli kriptografik algoritmaları belirli koşullar altında çalıştıran bir değerlendirme yazılımı kullanılmış olup yazılımın çıktıları sonrasında analiz edilmek üzere kayıt altına alınmıştır. Araştırmanın sonunda analitik süreç işletilerek oluşturulan bazı metrikler üzerinden karşılaştırmalar yapılmış ve sonuçları yorumlanmıştır.

Benzer alanda yapılmış çalışmalar Bölüm II'de, IoT cihazlarının seçim süreci Bölüm III'te, açık kaynaklı ücretsiz kriptografi kütüphanesi seçim süreci Bölüm IV'te, fiziksel test ortamının oluşturulması Bölüm V'te, değerlendirme(benchmark) yazılımının hazırlanışı ve yetenekleri Bölüm VI'da, ölçme süreci Bölüm VII'de

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on March 11,2024 at 16:39:34 UTC from IEEE Xplore. Restrictions apply.

anlatılmıştır. Son olarak değerlendirme yazılımı çıktılarının analiz edilip sonuçlarının yorumlandığı, gelecekteki çalışmalardan bahsedilen Bölüm VIII ile de makale sonuçlandırılmıştır.

II. KULLANIM

Makale ile ilgili konu başlıklarına geçmeden benzer alanlarda yapılmış çalışmalardan bahsetmek yerinde olacaktır.

"M-Ticarette ve Nesnelerin İnternetinde Enerji Duyarlı Güvenlik" başlıklı makalede en çok kullanılan şifreleme algoritmalarının güç ve kaynak tüketimine ilişkin bir değerlendirmesi yapılmıştır. Deneysel sonuçlar mobil cihazlarda şifreleme metodunun pil tüketimini etkilediğini göstermiştir. Bu nedenle, kullanıcıların verilen koşullar altında en uygun şifreleme yöntemini seçmelerini sağlayan, enerji açısından duyarlı olan bir politikaya sahip olmaları önemlidir [2].

"Simetrik Kriptografi Algoritmalarının Farklı Veri Türleri İçin Güç Tüketimi Üzerindeki Etkilerinin Değerlendirilmesi" başlıklı makalede AES, DES, 3DES, RC6, Blowfish ve RC2 şifreleme algoritmaları kullanılarak, belirli parametrelerin, güç tüketiminin de içinde bulunduğu bazı değerler üzerindeki etkisi araştırılmıştır. Etkisi test edilen bu parametreler sırasıyla paket boyutu değişimi, ses, video, resim dosya türlerinin her biri için tür değişimi, anahtar boyutu değişimidir. Araştırmanın sonucunda her bir algoritmanın performansı birbiri ile karşılaştırılmıştır. Güç tüketimi anlamındaki çıkarım ise anahtar boyutu artışının enerji tüketimini de arttırdığı yönündedir [3].

"Kriptografik Algoritmaların IoT Platformları ve İşletim Sistemleri üzerinde Performanslarının Değerlendirilmesi" başlıklı makalede, IoT ve WSN gibi platformlarda farklı güvenlik servisleri sağlayan simetrik kriptografik algoritmaların ayrıntılı bir değerlendirmesi sunulmuştur. Çalışmanın sonucunda veri girişi boyutuna bağlı olarak kriptografik algoritma önerilerinde bulunulmuştur [4].

IoT cihazları üzerinde kriptografik algoritmalar işletilerek cihazların performanslarının karşılaştırılmasına yönelik birçok makale [5][6] bulunmaktadır. Bu makalelerden bazıları ilerleyen başlıklar altında alıntılanmıştır.

III. IOT CİHAZLARININ SEÇİMİ

Üzerinde değerlendirme yazılımının çalıştırılıp ölçümlerin gerçekleştirileceği IoT cihazlarının seçimi araştırma açısından ciddi bir öneme sahiptir. Seçilecek cihaz sayısı iki adet olup bunlardan ilki IoT cihazları arasında görece performans anlamında güçlü, enerji verimliliği açısından zayıf bir cihaz olarak seçilmesi planlanmıştır. Aksi mantıkla seçilecek ikinci cihaz ise aynı sınıfta düşük performans, yüksek enerji verimliliği sunan bir model olarak seçilmiştir.

Yapılan açıklamalara uygun olarak, IoT ekosisteminde oldukça popüler, son tüketicinin yanında akademik çevrelerce de araştırmalarda sık sık tercih edilen Raspberry Pi ailesinden iki model seçilmiştir. Raspberry Pi Vakfı tarafından tasarlanıp üretimi sağlanan bu cihazlar Pi 3 Model B ve Pi Zero W modelleridir [7].

IV. KRİPTOGRAFİ KÜTÜPHANESİNİN SEÇİMİ

Sık kullanılan kriptografi algoritmalarını içeren bir test yazılımı hazırlamak için bu altyapıyı ücretsiz sunan ürünler araştırılmıştır. Araştırma sonucunda, popüler birçok kriptografi algoritmasını içeren ücretsiz, açık kaynak kodlu Crypto++ kütüphanesinin [8] kullanımına karar verilmiştir. C++ programlama dili kullanılarak geliştirilen bu kütüphane Linux tabanlı işletim sistemi yüklü olan Raspberry cihazlarında GCC derleyici ile derlenerek kolaylıkla kullanılabilmektedir.

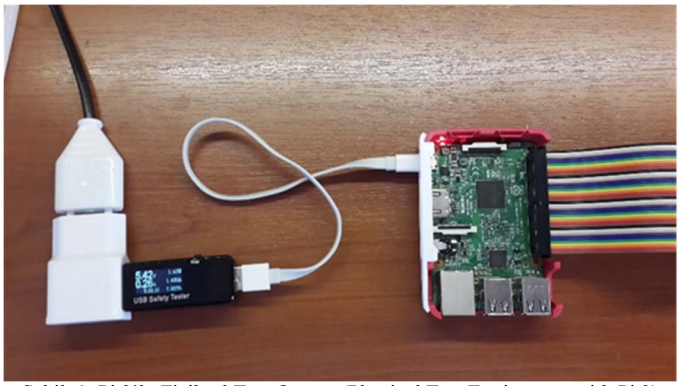
Crypto++ kütüphanesinin muadili ücretsiz yazılımlar arasından seçilmesinin başlıca nedeni, içeriğinde bir değerlendirme yazılımı barındırmasıdır. Bu değerlendirme yazılımı ihtiyaçlar doğrultusunda değiştirilip, üzerine eklemeler yapılarak nihai bir değerlendirme yazılımının ortaya çıkarılmasında ciddi bir katkı sağlamıştır. Değerlendirme yazılımın hazırlanması ile ilgili detaylar bir sonraki ana başlık altında anlatılacaktır.

Bilinirliği yüksek algoritmalardan kısaca bahsetmek gerekirse; simetrik şifreleme algoritması AES, blok şifresi olarak verileri gizlilik için şifrelemede kullanılır. RSA asimetrik algoritması sıklıkla dijital imza ve anahtar taşımada kullanılır. DH asimetrik anahtar anlaşmasında kullanılır. Bütünlük için SHA-1 ve SHA-256 kararlı hash algoritmaları kullanılmaktadır. Bir başka önemli asimetrik algoritma ECC daha kısa anahtar kullanımı ile eşit güvenlik sağlamada kullanılabilir [9].

V. FİZİKSEL TEST ORTAMININ HAZIRLANMASI

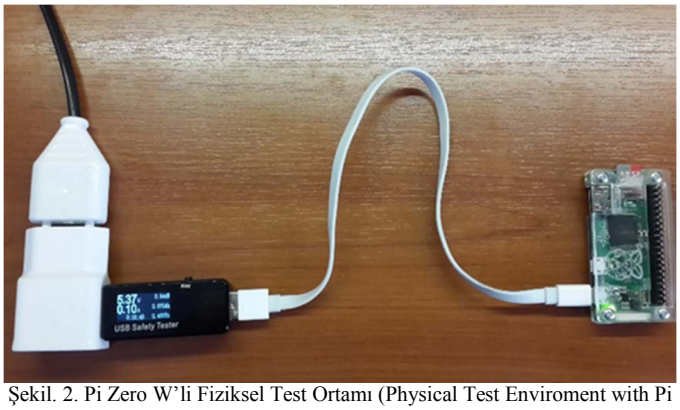
IoT cihazlarının enerji tüketim değerlerinin ölçülüp analiz edilebilmesi amacıyla fiziksel test ortamı hazırlanmıştır. Bu ortamda sırasıyla: 1 adet USB ölçüm cihazı, 1 adet 2m AC uzatma kablosu, 1 adet 2A akım çıkısını destekleyen USB sarj aleti, 1 adet 2A'lik akım geçişini destekleyen USB sarj kablosu ve son olarak da 2 adet Raspberry Pi cihazı bulunmaktadır.

Test ortamında en kritik görevi üstlenen USB ölçüm cihazı, USB adaptör ile IoT cihazı arasında konumlandırılmakta ve adaptör tarafından beslenen IoT cihazının enerji tüketimine yönelik metrikler sunmaktadır. IoT cihazını beslemek için şebeke beslemeli USB şarj aleti kullanılmıştır. İlgili bağlantı kabloları da cihazlar arasında kullanılmıştır. Hazırlanan test ortamları sırasıyla Şekil 1 ve Şekil 2'de gösterilmiştir.



Şekil. 1. Pi 3'lü Fiziksel Test Ortamı (Physical Test Enviroment with Pi 3)

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on March 11,2024 at 16:39:34 UTC from IEEE Xplore. Restrictions apply.



Şekil. 2. Pi Zero W'li Fiziksel Test Ortamı (Physical Test Enviroment with Pi Zero W)

Fiziksel bir ölçüm cihazı kullanmak yerine IoT cihazı üzerinden yazılım tabanlı ölçüm yapılması konusu araştırılmış ve fiziksel bir ölçüm cihazı kullanılmasına karar verilmiştir. Nedeni ise; bu tip ölçümlerde, ölçümün ilgili cihaz üzerindeki işletim sisteminde koşan bir yazılım vasıtasıyla yapılması, bazı metriklerin ölçümlenememesi; ayrıca ölçümlenebilen değerlerin ise donanımsal ölçüm yapan cihazlara nazaran hassasiyet ve doğruluk açısından düşük sonuçlar vermesidir.

VI. Değerlendirme Yazılımı

Değerlendirme yazılımı üzerinde ihtiyaçlar doğrultusunda yapılan değişiklikleri aşağıda sıralanmıştır:

- Her algoritma sınıfından en az bir algoritma olması koşuluyla popüler olanlara öncelik verilerek değerlendirilen algoritma sayısı azaltılmıştır. Araştırmanın amacı algoritmaların performans verilerini karşılaştırmak değil, cihazların bu algoritmaları işletirken harcadığı enerji tüketimlerini karşılaştırmak olduğu için bu değişikliğe gidilmiştir.
- USB ölçüm cihazının çıktılarını kullanıcı girişiyle klavyeden alan yapı eklenmiştir. Bu metrikler sırasıyla Ah (amper-saat) ve Wh (watt-saat)'dir.
- Her bir algoritmanın işletilme süresini milisaniye hassasiyetinde ölçen yapı değerlendirme yazılıma eklenmiş, bu süre analiz sürecinde kullanılmak üzere metrikler arasına alınmıştır.
- Algoritma işletimleri arasına duraklatma mekanizması konulmuştur.
- Ölçüm sürecinde konsol üzerinden kullanıcıya hangi algoritma üzerinde işlem yapıldığı bilgisini paylaşan ek bilgi mekanizmaları eklenmiştir.
- Değerlendirme yazılımı çıktılarını web tarayıcısı üzerinden okunabilen tablo formatı halinde sunmaktadır. Bu tabloya değerlendirme yazılımına sonradan eklenen tüm metrikler de dahildir.

Yapılan bu değişiklikler neticesinde fiziksel test ortamı ile tam uyumlu bir değerlendirme yazılım ortamı hazırlanmış olmaktadır.

VII. Performans Karşılaştırılması

A. Ölçümlerin Yapılması

Ölçümlenmesi gereken bilgi, aynı kriptografik algoritmayı işletirken cihazların tükettiği enerji miktarıdır. Kullanılan birim Wh (watt-saat) olup birim zamanda tüketilen enerjiyi ifade etmek için kullanılır. Amaç, değerlendirilmesi gereken her bir algoritmanın işletildiği *süre* boyunca tükettiği enerji değerinin hesaplanmasıdır. Ölçme adımları sıralamak gerekirse:

- Yazılım başlatılır. Yazılım her bir algoritma işletimi öncesi akışı duraklatır ve devam etme kontrolünü kullanıcıya bırakır.
- Algoritmanın işletilmeye başlamasıyla beraber kullanıcı tarafından USB ölçüm cihazı üzerindeki sıfırlama tuşuna basılır ve ölçme işlemine başlanılır.
- Ölçme tamamlandığında yazılım kullanıcıdan ölçülen Wh değerinin girmesini ister. Kullanıcı da USB ölçüm cihazının ekranından okuduğu değeri yazılıma girer.
- Her bir algoritma için ikinci ve üçüncü adımlar tekrar edilir.
- Değerlendirme yazımı kendi ölçümleri ve kullanıcıdan aldığı ölçümleri birleştirerek çıktıları tablo formatında ".htm" dosyasına basar ve böylelikle değerlendirme süreci tamamlanmış olur.

B. Ölçümlerin Değerlendirilmesi

Değerlendirme yazılımının çıktıları sırasıyla MiB/Second ve Operation/Second'dır. MiB/Second, bir saniyede cihaz tarafından üretilebilen Mebibyte(1024B x 1024B) miktarını ifade eder. Operation/Second ise bir saniyede cihaz tarafından ilgili algoritma için işletilen kriptografik operasyon (işlem döngüsünü) sayısını ifade eder.

Elde edilen çıktılar ile karşılaştırmayı sağlayacak metrikler elde edilmeye çalışılmıştır. Bu metrikler sırasıyla µWh/MiB ve µWh/Operation'dir. µWh/MiB, ilgili algoritma kullanılarak cihazın bir MiB veriyi işlemek için harcaması gereken enerjiyi µWh cinsinden ifade eder. µWh/Operation ise ilgili algoritma kullanılarak cihazın bir operasyonu (işlem döngüsünü) tamamlaması için harcaması gereken enerjiyi µWh cinsinden ifade eder.

VIII. Sonuç ve Gelecek Çalışmalar

Tablo I ve Tablo II'deki sonuçlar yorumlandığında, performans açısından Pi 3 ile Pi Zero arasında beklenildiği gibi Pi 3 ün önde olduğu bir sonuç ortaya çıkmıştır. Bu oran yaklaşık iki kattır. Cihaz işlemcileri arasındaki donanımsal farkın bu sonucu ortaya çıkardığı söylenebilir.

µWh/MiB metriğinin kullanıldığı algoritmaların gruplandığı Tablo I'de Pi 3'ün benzer işlemi gerçekleştirirken birçok algoritmada az bir farkla daha fazla enerji tükettiği görülmüştür. µWh/Operation metriği üzerinden hesaplamaların yapıldığı algoritma grubunu içeren Tablo II'de ise Pi Zero'nun az farkla enerji tüketimi fazla olan tarafta olduğu görülmüştür.

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on March 11,2024 at 16:39:34 UTC from IEEE Xplore. Restrictions apply.

TABLO I. ALGORİTMA GRUBU I PERFORMANS VE ENERJİ TÜKETİMİ SONUÇLARI (ALGORİTHM GROUP I PERFORMANCE AND ENERGY CONSUMPTİON RESULTS)

Algoritma Grubu I Performans ve Enerji Tüketimi Sonuçları	**Performans MiB/Second**		**Güç Tüketimi µWh/MiB**	
	Pi 3 Model B	***Pi Zero W***	***Pi 3 Model B***	***Pi Zero W***
AES/CTR (128-bit key)	21	12	29,01	26,62
AES/CTR (256-bit key)	16	9	38,20	31,60
AES/GCM (2K tables)	13	7	45,16	43,55
AES/GCM (64K tables)	14	6	42,28	41,79
Blowfish/CTR (128-bit key)	31	16	18,46	17,79
DES/CTR (64-bit key)	17	8	33,58	24,80
DES-EDE3/CTR (192-bit key)	7	3	86,31	92,69
DES-XEX3/CTR (192-bit key)	15	8	37,92	36,62
IDEA/CTR (128-bit key)	21	11	28,62	23,98
MD5	185	93	3,18	2,94
RC5 (r=16)	34	17	16,81	17,19
RC6/CTR (128-bit key)	38	17	15,79	16,00
SHA-1	89	41	6,34	6,86
SHA-256	43	20	13,59	13,91
SHA3-256	8	4	72,61	67,52
SHA3-512	4	2	146,39	143,37
SHA-512	14	7	42,32	37,25
Twofish/CTR (128-bit key)	35	17	17,40	16,07
Whirlpool	5	3	120,12	98,96

TABLO II. ALGORİTMA GRUBU II PERFORMANS VE ENERJİ TÜKETİMİ SONUÇLARI (ALGORİTHM GROUP II PERFORMANCE AND ENERGY CONSUMPTİON RESULTS)

Algoritma Grubu II Performans ve Enerji Tüketimi Sonuçları	**Performans Operation/Second**		**Güç Tüketimi µWh/Operation**	
	Pi 3 Model B	***Pi Zero W***	***Pi 3 Model B***	***Pi Zero W***
DH 1024 Key Agreement	207,90	64,68	2,73	4,12
DH 1024 Key-Pair Generation	312,50	81,90	1,92	2,85
DH 2048 Key Agreement	55,65	20,28	10,18	13,12
DH 2048 Key-Pair Generation	70,18	24,51	8,55	10,87
DSA 1024 Signature	317,46	83,47	1,78	2,80
DSA 1024 Verification	281,69	73,86	2,01	3,61
ECDSA over GF(2^n) 233 Signature	43,08	24,32	13,15	10,96
ECDSA over GF(2^n) 233 Verification	34,27	19,62	16,52	15,28
ECDSA over GF(p) 256 Signature	125,00	59,45	4,53	4,49
ECDSA over GF(p) 256 Verification	48,10	24,18	12,47	12,40
RSA 1024 Decryption	144,93	31,46	3,91	7,42
RSA 1024 Encryption	3571,43	1149,43	0,17	0,23
RSA 1024 Signature	144,93	31,96	4,14	7,30
RSA 1024 Verification	3571,43	1204,82	0,16	0,22
RSA 2048 Decryption	24,87	6,60	24,10	40,40
RSA 2048 Encryption	1470,59	568,18	0,41	0,47
RSA 2048 Signature	24,74	6,70	25,57	39,80
RSA 2048 Verification	1492,54	588,24	0,38	0,45
XTR-DH 342 Key Agreement	53,08	10,11	11,29	23,03
XTR-DH 342 Key-Pair Generation	105,15	20,15	5,71	13,22

Bütün algoritmalar göz önüne alındığında ortalama enerji tüketimi açısından cihazların birbirine yakın değerler ortaya çıkardığı söylenebilir. Pi Zero'nun birim operasyon üzerinden enerji tüketimi hesabıyla değerlendirme yapılan algoritmalarda daha fazla enerji tüketen taraf olarak gözlenmesi bu algoritmaların yapısının, dört çekirdeğe sahip Pi 3 modelinde işletilmeye daha uygun olmasından kaynaklıdır. Pi Zero modelinin enerji verimliliği yüksek bir cihaz olmasına karşın enerji tüketimi sonuçlarında Pi 3 ile yakın sonuçlar elde etmesinin nedeni de performansına bağlı olarak birim zamanda daha az iş yapmasından kaynaklıdır.

Sonuç olarak, fiyat açısından aralarında üç buçuk kata yakın fark bulunan, yapılan sentetik testler ile performans olarak da aynı yönde iki kata yakın farkın görüldüğü bu cihazların kriptografik algoritmalar kullanılarak enerji tüketimleri karşılaştırıldığında aralarında düşük miktarda farkların çıktığı sonuçlar görülmüştür. Bunun bir sonucu olarak enerji kritik işlemler yapılırken diğer gereksinimlere bağlı karar verilmesi daha doğru olacaktır. Örneğin maliyet odaklı bir çözüm aranıyorsa Pi Zero modeli, aksine performans odaklı bir çözüm aranıyorsa Pi 3 modeli yönünde bir tercih yapılabilir.

Gelecek çalışmalar olarak, aynı uygulanmanın çok daha hassas sonuçlar verebilmesi adına test sürecinde kullanıcı kontrolünde olan ve kullanıcı reaksiyonları ile gerçekleşen işlemlerin otomatikleştirilmesi üzerine çalışılabilir. Örneğin USB ölçüm cihazı üzerinden kullanıcı tarafından okunarak alınan ölçüm değerlerinin yerine bu işlemin yazılım tarafından otomatik okunması sağlanabilir. Ayrıca ileride değerlendirme yapılan IoT cihaz çeşitliliği arttırılarak hem araştırmanın geçerliliği pekiştirilmiş olur hem de sonuçlar üzerindeki yorumlar zenginleştirilebilir. Son olarak ölçümler yapılırken cihazların çalışmak zorunda olmayan donanımları ve çıkış portları kapatılması ve konsol tabanlı (GUI'si olmayan) bir işletim sistemi kullanılması üzerine çalışılabilir. Böylece ölçümlenen güç tüketimleri bir miktar daha aşağıya çekilebilir.

BİLGİLENDİRME

Bu araştırma Aselsan A.Ş. Savunma Sistem Teknolojileri Sektör Başkanlığı tarafından desteklenmiştir.

KAYNAKLAR

[1] Web, https://www.raspberrypi.org/about/

[2] Hamad, Fadi, Leonid Smalov, and Anne James. "Energy-aware Security in M-Commerce and the Internet of Things." IETE Technical review 26.5 (2009): 357-362.

[3] Minaam, Diaa Salama Abdul, Hatem Mohamed Abdual-Kader, and Mohiy Mohamed Hadhoud. "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types." IJ Network Security 11.2 (2010): 78-87.

[4] Pereira, Geovandro CCF, et al. "Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems." Security and Communication Networks 2017 (2017).

[5] Dinu, Daniel, et al. Triathlon of lightweight block ciphers for the internet of things. IACR ePrint archive, 2015.

[6] Beaulieu, Ray, et al. "SIMON and SPECK: Block Ciphers for the Internet of Things." IACR Cryptology ePrint Archive 2015 (2015): 585.

[7] Web, https://www.raspberrypi.org/products/

[8] W. Dai, "Crypto++ 5.6.5 Benchmarks", http://www. cryptopp.com/ benchmarks.html, 2016.

Authorized licensed use limited to: b-on: Instituto Politecnico de Lisboa. Downloaded on March 11,2024 at 16:39:34 UTC from IEEE Xplore. Restrictions apply.