DAR BANT NESNELERİN İNTERNETİ UYGULAMALARINDA VERİ GÜVENLİĞİ

Uygar İşiçelik
171405102
Orcid: 0000-0001-7239-7578

YÜKSEK LİSANS TEZİ
Elektrik-Elektronik Mühendisliği Anabilim Dalı
Elektrik-Elektronik Mühendisliği Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Fatma Sarıca

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Eylül, 2021



JÜRİ VE ENSTİTÜ ONAYI

Bu belge, Yükseköğretim Kurulutarafından 19.01.2021 tarihli *"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"* ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulutarafından 19.01.2021 tarihli *"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"* ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

TEŞEKKÜR

Bu çalışmada bilgi ve tecrübesi ile beni destekleyen ve yardımcı olan değerli danışman hocam Dr. Öğr. Üyesi Fatma Sarıca'ya teşekkürü borç bilirim.

Yüksek Lisans eğitimim boyunca maddi ve manevi beni destekleyen aileme ve eşime sevgi ve saygılarımı sunarım.

Uygar İşiçelik

Eylül, 2021

ÖZ

DAR BANT NESNELERİN İNTERNETİ UYGULAMALARINDA VERİ GÜVENLİĞİ

Uygar İşiçelik
Yüksek Lisans Tezi
Elektrik-Elektronik Mühendisliği Anabilim Dalı
Elektrik-Elektronik Mühendisliği Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Fatma Sarıca
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2021

Hayatımızın her alanına dahil olan akıllı cihazların temelinde Nesnelerin İnterneti kavramı vardır. Bu kavram günümüzde uzaktan izlenebilen – yönetilebilen akıllı cihazlar olarak aktarılsada bir çok son tüketici ve endüstriyel ürünlerin temel katmanlarından birisi haline gelmiştir. İnternete bağlı olan cihaz sayılarımızın artması birden fazla konularda araştırma ve geliştirme ihtiyacı doğmuştur. Bu konulardan en yaygın olanı artan cihaz sayısına karşın ihtiyaç duyulan enerji ve internete bağlı olan cihazlarımızın uzak sunuculara gönderdiği ve sakladıkları verilerin güvenliğidir. Gelişen üretim teknolojileri ile düşük güç tüketimli işlemcilerin pazara sunulması, kablosuz enerji hasadı, enerji depolama gibi alternatif çözümlerin yaygınlaşmasıyla birlikte enerji ihtiyacı kontrol edilebilir, ölçeklenebilir olacaktır. Kullanıcı verisi ise her üreticinin kendine özgü yöntemler ile sakladığı, kullandığı bir bilgidir. Bu çalışmada Nesnelerin İnterneti kavramında yeni olan Dar Bant Nesnelerin İnterneti (NB-IoT, Narrow Band Internet of Things) ile çalışan sayaç otomasyonu uygulaması geliştirilmesi, sayaç verilerini sahte isim, soyisim, adres, cinsiyet gibi veriler ile eşleştirip, verilerin uluslararası kişisel verilerin korunması kapsamında güvenliği irdelenmiştir.

Çalışmada Raspberry-Pi donanımı ile sayaç verileri okunup, sayaca ait veriler kişi ile eşleştirilip uzak sunucuda saklanılması amaçlanmıştır. Bu çalışma ile hem donanım seviyesinde hem de yazılım seviyesinde kayıt edilen verilerin güvenliği irdelenmiştir.

Anahtar Sözcükler: NB-IoT; Dar Bant Nesnelerin İnterneti; Nesnelerin İnterneti; M-Bus; Veri Güvenliği; iOS Mobil Uygulama.

ABSTRACT

DATA SECURITY IN NARROW BAND INTERNET OF THINGS APPLICATIONS

Uygar İşiçelik
Master Thesis
Department of Electrical and Electronics Engineering
Electrical and Electronics Engineering Programme
Thesis Advisor: Asst. Prof. Fatma Sarıca
Maltepe University Graduate School, 2021

The concept of the Internet of Things forms the basis of smart devices, that we use in all areas of our lives. Although this concept is considered as smart devices that can be monitored and managed remotely, it has become one of the basic layers of the many end-user and industrial products. The increase in the number of devices connected to the Internet has created a need for research and development in more than one area. One of the most common of these issues is the increase in the energy needed with the increasing number of devices and the security of the data that Internet-connected devices send and store to remote servers. With the introduction of low-power consumption processors to the market with the developing production technologies, and the spread of alternative solutions such as wireless energy harvesting and energy storage, the energy need will become controllable and scalable. User data, on the other hand, is the information that each manufacturer stores and uses with its own methods. In this thesis, meter automation application working with Narrow Band Internet of Things (NB-IoT, Narrow Band Internet of Things), which is the new concept of Internet of Things, has been developed. By matching the meter data with fake name, surname, address, gender, the security of the data within the scope of the international personal data protection law has been examined.

In the thesis, it is aimed to read the meter data with Raspberry-Pi hardware, to match meter data with the fake people created and to store it on the remote server. The security of the data recorded at both the hardware level and the software level has been examined.

Keywords: NB-IoT; Narrow Band Internet Of Things; M-Bus; Data Security; iOS Mobile Application.

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ii
ETİK İLKE VE KURALLARA UYUM BEYANI iii
TEŞEKKÜR iv
ÖZ v
ABSTRACT vi
İÇİNDEKİLER vii
TABLOLAR LİSTESİ viii
ŞEKİLLER LİSTESİ ix
KISALTMALAR x
ÖZGEÇMİŞ xi
BÖLÜM 1. GİRİŞ 1
BÖLÜM 2. NESNELERİN İNTERNETİ 4
2.1. Dar Bant Nesnelerin İnterneti 4
2.2. Veri İletim Protokolleri 6
2.2.1. TCP Soket 6
2.2.2. UDP Soket 7
BÖLÜM 3. METER-BUS PROTOKOLÜ 9
3.1. M-Bus İletişim 10
3.1.1. Master to Slave (M2S) İletişim 10
3.1.2. Slave to Master (S2M) İletişim 11
BÖLÜM 4. RASPBERRY-PI 13
4.1. Raspberry Pi Donanım Özellikleri 15
BÖLÜM 5. YÖNTEM 15
5.1. M-Bus Destekli Sayaçlar 16
5.2. mBus - USB Dönüştürücü Donanımı 17
5.3. Quectel BC96 NB-IoT Geliştirme Kiti 19
5.4. Raspberry Pi - Sayaç Okuma Uygulaması 19
5.5. iOS Mobil Uygulama – Sayaç Verileri İzleme Uygulaması 20
5.6. Uzak Sunucu Bileşenleri 23
5.5.1. Veritabanı 23
5.5.2. Arka Uç Uygulaması 24
5.7. Veri Güvenliği Kapsamında Yapılan Çalışmalar 25
5.8. Atak Yöntemleri 27
5.8.1. Man in the Middle (MitM) Saldırısı 27
5.8.2. Denial-of-Service (DoS) Saldırısı 27
5.8.3. Replication Saldırısı 27
BÖLÜM 6. BULGULAR VE YORUMLAR 29
6.1. Sisteme Genel Bakış 29
BÖLÜM 7. SONUÇLAR 31
KAYNAKÇA 33

TABLOLAR LİSTESİ

Tablo 2.1. TCP Socket Uygulamaları 7

Tablo 4.1. Raspberry Pi Donanım Özellikleri..... 15

Tablo 5.1. PMM-10 Donanım Özellikleri [7] 17

ŞEKİLLER LİSTESİ

Şekil 2.1. Bant Genişliği - Kapsama Alanı Grafiği 6

Şekil 3.1. M-Bus M2S İletişimi Sırasında Gerilim ve Akım Grafiği 11

Şekil 3.2. M-Bus S2M İletişimi Sırasında Gerilim ve Akım Grafiği 12

Şekil 4.1. Raspberry Pi 4 14

Şekil 5.1. M-Bus Sayaç Seri No Bilgisi 17

Şekil 5.2. PMM-10 Bağlantı Şeması 18

Şekil 5.3. MBSheet Uygulaması ile Sayaç Değerleri Görüntülenmesi 18

Şekil 5.4. Quectel BG96 Geliştirme Kiti 19

Şekil 5.5. Java Uygulaması Okuyucu Planlama ve Çalıştırma Fonksiyonları 20

Şekil 5.6. Giriş İstek Örneği ve accessToken Değeri 21

Şekil 5.7. Yetkisiz İstek Talebi 22

Şekil 5.8. iOS Uygulama Ekran Görüntüleri 22

Şekil 5.9. Giriş ve Sayaç Değerlerinin Fonksiyonları 23

Şekil 5.10. Veritabanı İlişkisel Diagramı 24

Şekil 5.11. Raspberry Pi Periyot Fonksiyonları 25

Şekil 5.12. Telemetri Servisi ve Veritabanı Kayıt Fonksiyonu 25

Şekil 6.1. Sistemin Genel Akışı 30

Şekil 7.1. SonarQube Kod Analizi ve Kod Güvenliği Sonucu 32

KISALTMALAR

IoT : Internet of Things, Nesnelerin İnterneti

IIoT : Industrial Internet of Things, Endüstriyel Nesnelerin İnterneti

NB-IoT : Narrow Band Internet Of Things, Dar Bant Nesnelerin İnterneti

M-Bus : Meter Bus

M2S : Master to Slave

S2M : Slave to Master

iOS : iPhone Operating System

TCP/IP : Transmission Control Protocol / Internet Protocol

UDP : User Datagram Protocol

TLS : Transport Layer Security

SSL : Secure Socket Layer

UART : Universal Asynchronous Receiver Transmitter

REST : Representational State Transfer

API : Application Programming Interface

JWT : JSON Web Token

ÖZGEÇMİŞ

Uygar İşiçelik

Elektrik Elektronik Mühendisliği Anabilim Dalı

Eğitim

Y.Ls.	2017	Maltepe Üniversitesi, Lisansüstü Eğitim Enstitüsü Elektrik Elektronik Mühendisliği Anabilim Dalı
Ls.	2010	Girne Amerikan Üniversitesi, Mimarlık & Mühendislik Fakültesi Elektrik Elektronik Mühendisliği
Lise	2006	Özel Toros Fen Lisesi

İş/İstihdam

2021 Kıdemli Yazılım Mühendisi, Huawei
2019 - 2021 Deneyimli Yazılım Uzmanı, Akbank
2018 - 2019 Yazılım Geliştirici, Meyer Grup
2015 - 2018 Ar-Ge Mühendisi, RTM Elektronik

Mesleki Birlik/Dernek Üyelikleri

2016 - Üye: Google Geliştiriciler Grubu, İstanbul
2015 - Üye: Elektrik Mühendisleri Odası, İstanbul

Alınan Burs ve Ödüller

2010 - Girne Amerikan Üniversitesi Eğitim Bursu

BÖLÜM 1. GİRİŞ

Nesnelerin İnterneti kavramı elektronik, yazılım, üretim teknolojileri, yapay zeka, endüstriyel otomasyon gibi birçok disiplini içinde barındıran geniş bir kavramdır. Günümüzde kullandığımız akıllı cep telefonları, akıllı saatler, ev otomasyon sistemleri, uzaktan izleme sistemleri gibi kablolu / kablosuz farketmeksizin internet ağına bağlanabilen, veri toplayabilen, topladığı verileri sizin için işleyebilen donanım, yazılım bütünüdür.

Son tüketici ürünleri dışında devlet kurumları için bazı şehirlerde kullanılmaya başlanan olan akıllı şehir uygulamaları da Nesnelerin İnterneti uygulamalarına dahil olmaktadır. Son tüketici uygulamaları ve akıllı şehir uygulamaları birleştiğinde cep telefonunuz, akıllı asistanınız size trafiğin arttığını ve günlük rutininizden daha erken yola çıkmanız gerektiğini belirten bir bildirim göndermesi örnek olarak gösterilebilir.

Aynı zamanda akıllı saatlerin hayatımıza dahil olmasıyla birlikte sensörler aracılığıyla kalp atış hızı, elektrokardiyografi, kanda bulunan oksijen değeri gibi sağlık verilerini toplayıp doktorunuza sunmaya olanak sağlamaktadır.

Son tüketici hedefli uygulamaların yanında Nesnelerin İnterneti uygulamaları endüstride de oldukça geniş bir yer tutmaktadır. Endüstride kullanılan sensör, otomasyon ürünlerinin makine öğrenimi, uzak sunucu ile çalışabilirliğinin sağlanması ile üretim ve sanayi sektörlerinin farklı alanlarında nesnelerin interneti uygulamaları için ticari yatırımlar yapılmaktadır. 4. Sanayi Devrimi olarak da duyduğumuz Endüstri 4.0, sanayide nesnelerin interneti uygulanması kullanılarak operasyon ve üretim süreçlerinde verimliliği arttırmayı hedeflemektedir.

Uygulamalar, son tüketiciye veya endüstride faydalı olsada bazı güvenlik sorunlarını beraberinde getirmektedir. Üreticiler, akıllı cihazların topladıkları verileri işlemek veya tüketiciye geçmişe dönük verileri göstermek için bu verileri saklarlar bu veriler tüketicinin kişisel bilgileri olduğu gibi bazı kullanım alışkanlıklarını da

saklayabilir. Örneğin akıllı ev sistemi kullanan bir tüketici, haftaiçi 08:00 ve 19:00 saatleri arasında evde olmadığının bilgisini girişte bulunan varlık sensörü aracılığı ile vermiş olmaktadır. Farklı bir akıllı saat kullanıcısı gün içinde ne kadar süre hareketsiz kaldığı bilgisini de üreticiye veya uygulama sahibine vermiş olmaktadır.

Bu verilerin sızması veya çalınması durumunda üçüncü kişilere isim, soyisim, cep telefonu gibi erişilebilir bilgilerinizin yanında alışkanlıklarınızı da ele geçirmektedirler. Bu bilgiler bir güvenlik şirketinin eline geçtiğinde tüketiciyi arayarak 08:00 – 19:00 saatleri arasında güvenlik hizmeti sunabileceğini, aynı şekilde bir spor salonu diğer tüketiciyi arayarak spor aboneliği teklifi sunmak isteyebileceğini, bir sağlık sigortası şirketi ise bu tüketicinin hareketsiz olması nedeniyle ekstra muayne şartları veya tüketiciyi daha fazla prim ödemeye mecbur bırakabilir. Bu nedenler ile akıllı cihazlardan ve tüketicilerden elde edilen verilerin nesnelerin interneti uygulamasında güvenli bir şekilde kayıt altına alınmalıdır.

Literatürde IoT uygulamalarının farklı mimari katmanlarında karşılaşılabilecek güvenlik ve gizlilik risklerinin tanımlanması, incelenmesi ve olası açıklara karşı güvenlik ve gizlilik zaafiyetlerinin minimuma indirilmesine yönelik yapılmış çeşitli çalışmalar vardır.

Yang ve diğerleri tarafından yapılmış çalışmada IoT atakları ve güvenlik mekanizmalarının sınıflandırılması üzerinde durulurken IoT uygulamalarda kimlik doğrulama şemaları ve mimarileri üzerine yapılan çalışmaların incelenmesi sunulmuştur [1].

Chen ve diğerleri tarafından yapılan çalışma da ise spesifik olarak IoT tabanlı servislere özgü güvenlik konusunu ele alınmıştır. Bu çalışma içerisinde sağlam, gizlilik ve güvenliği koruyan konumlandırma tabanlı hizmetler sunan IoT sistemler için belirli şifreleme çözümlerine yer verilmiştir [2].

IoT orta katmanındaki güvenlik sorunlarına yönelik bir çalışma ise Ngu ve diğerleri tarafından sunulmuştur. Çalışma içerisinde mevcut protokoller ve protokollere ait güvenlik sorunlarına dair araştırmalar sunulmuştur. Çalışma IoT cihaz ve uygulama arasındaki ara katmanda yani orta katman yazılımı geliştirilmesinde IoT sistemlerindeki

heterojen yapının sağlanırken aynı zamanda temel bileşen olan güvenliğin desteklemesine dair kapsamlı analiz sunmaktadır [3].

Farris ve diğerlerinin yaptığı IoT sistemlerde yazılım tabanlı iletişim ve ağ fonksiyonlarının sanallaştırılması çalışmasında IoT cihazlara, bulut platforma ve IoT uygulamalara yapılan donanım çoğaltılması, zararlı yazılım yüklenmesi, Denial-of-Service (DoS) atağı, yönlendirme manipülasyonu gibi 19 farklı atak türlerine güvenlik duvarı, şifreleme, yetkilendirme gibi önlemlerin etkisi araştırılmıştır [4].

Zhan ve diğerlerinin NB-IoT üzerinde yapmış olduğu şifreleme çalışması ile son kullanıcı, cihaz ve uygulama katmanlarında çözücü şifrelerin belirli bölümleri saklanarak güvenli ağ iletişimi, veri güvenliği, veri bütünlüğü doğrulaması sağlanmıştır. Bu çalışma ile NB-IoT uygulamalarında şifreleme konusunda ileriye dönük fikirler ortaya koymaktadır [5].

Çalışmanın devamında 2. Bölüm içerisinde Dar Bant Nesnelerin İnterneti, sistem bileşenleri ve mimarileri genel olarak incelenmiştir. 2. Bölümün devamında ise verilerin iletimi için tercih edilmiş olan Representation State Transfer (REST) protokolüne değinilmiştir. 3. Bölümde ise çalışmada kullanılacak olan sayaç otomasyonunda kullanılan uluslararası sayaç okuma protokollerine ayrılmıştır. 4. Bölüm ile çalışmanın uçtan uca mimarisi, mimari üzerinden oluşabilecek veri sızıntılarının önüne geçilmesi için yapılabilecek çalışmalar, sayaç okuma yazılımı, verilerin kaydedilmesi için veritabanı oluşturulması, iOS mobil uygulama ortamında kullanıcıya verilerin güvenli şekilde iletilmesi incelenmiştir. 5. Bölüm içerisinde sisteme genel bir bakış, sistem analizine yer verilmiştir. Son olarak 6. Bölüm içerisinde açık kaynaklı sızma testleri ile uygulamaya sızma testi uygulayıp uygulamanın güvenilirliği test edilip sonuçları paylaşılmıştır.

BÖLÜM 2. NESNELERİN İNTERNETİ

Procter & Gamble firmasının çalışanı olan Kevin Ashton, 1999 yılında tedarik zincirlerinde yaşanan problemi çözmek için RFID ve interneti kullanılarak çözüm olabileceğini düşündüğü bir sunumda Nesnelerin İnterneti kavramını kullanmıştır.

Uluslararası Telekomünikasyon Birliği'nin (ITU) yaptığı tanım ise nesnelerin veya cihazların herhangi bir zamanda ve herhangi bir ortam bağımlılığı olmadan birbirleriyle bağlantıda olabileceği teknolojidir.

Üretim teknolojilerinin artmasıyla birlikte gelişen düşük güç tüketimli işlemciler, sensörler, bağlantı arayüzleri ile donatılmış akıllı telefonlar, akıllı televizyonlar, akıllı saatler nesnelerin interneti uygulamalarına uygun örneklerdir.

Uygulamada, nesnelere eklenen sensörler ortamdaki (Örneğin sıcaklık, nem, pH, oksijen miktarı vb.) veya kişiye ait parametreleri izleme (Örneğin kalp atış hızı, kandaki oksijen miktarı vb.) ve bu verileri saklama özelliği kazandırılabilir. Aynı zamanda sahip oldukları bağlantı arayüzleri sayesinde nesneler kendi aralarında internet bağımlılığı olmadan konuşabilir, uzak sunucu aracılığıyla bir nesneye iletilen mesajın ağda bulunan diğer nesnelere iletilmesi mümkün olmaktadır.

2.1. Dar Bant Nesnelerin İnterneti

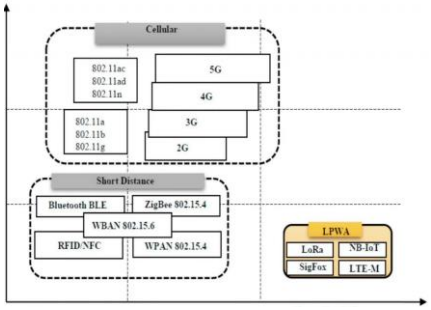
Nesnelerin interneti uygulamalarında gereksinimlere göre farklı yazılım ve donanım teknolojileri kullanılır. Örneğin akıllı şehir uygulamaları için canlı veri çok kritik iken akıllı ev uygulamaları için aynı özellik olmayabilir. Aynı zamanda nesneler internete bağlanma arayüzleri, birden fazla nesnenin birbiri ile iletişim kurması gibi ihtiyaçlara karşın farklı teknolojiler ortaya çıkmıştır. Bu nedenle nesnelerin interneti uygulamalarında standart mimari bulunmamaktadır.

Nesnelerin İnterneti uygulamalarında yaygın olarak

- Wi-Fi
- Hücresel – 2G, 3G, 4G, 5G
- Low Power Wide Area Networks (LPWAN)
- Bluetooth Low Energy (BLE) & Bluetooth
- Radyo Frekansı & Mesh

teknolojileri kullanılmaktadır. Bu teknolojiler arasında Wi-Fi ve hücresel bağlantı arayüzünü içeren nesneler internete direk erişim sağlayabilirken diğer arayüzler veriyi internet aracılığı ile iletmek için Wi-Fi veya hücresel arayüzünü kullanan ağ geçidine ihtiyaç duymaktadırlar.

Bu bağlantı çeşitlerin arasında 2016 yılında 3rd Generation Partnership Project (3GPP) tarafından tanıtılan Dar Bant Nesnelerin İnterneti (Narrow Band Internet of Things – NB-IoT) hem hücresel özelliği hemde düşük güç tüketimli geniş alan ağları oluşturmaktadır. NB-IoT'nin isminin dar bant olması hücresel (ses & internet) ağların kullandığı frekans bantlarını kullanmaması ve hücreselde kullanılan frekans aralığının çok altında frekans bantlarına sahip olması en önemli özelliğidir. Düşük frekans kullanılarak tek baz istasyonu ile daha uzak mesafelere ve daha fazla nesneler ile iletişim kurması en önemli özelliğidir. Diğer teknolojiler ile kıyaslanan bant genişliği ve kapsama alanı grafiği Şekil 2.1'de gösterilmiştir.



Şekil 2.1. Bant Genişliği - Kapsama Alanı Grafiği

NB-IoT'nin önemli olmasının en büyük nedenlerinden birisi de önümüzdeki yıllarda 2G baz istasyonları kaldırılması nedeniyle ortaya çıkacak Makine – Makine (M2M) iletişimlerinin yerine birebir geçebilecek daha ucuz maliyetli bir teknoloji olmasıdır.

Ülkemizde, Turkcell ve Vodafone belirli kotalarda ve belirli müşterilere NB-IoT erişimi sağlamaktadır.

2.2. Veri İletim Protokolleri

Nesneler, elde ettiği verileri uzak sunucuya belirli protokoller aracılığıyla yapar bu protokollerin en alt katmanında Transmission Control Protocol (TCP) veya User Datagram Protocol (UDP) soketleri bulunmaktadır.

Nesnelerin interneti uygulamalarında kullanılan Message Queue Telemetry Transport (MQTT), Representational State Transfer (REST) gibi uygulama katmanı seviyesinde bulunan bütün uygulamalar bu soket yapılarını kullanmaktadır.

2.2.1. TCP Soket

TCP protokolü bağlantı temelli bir protokoldür. Nesne veriyi uzak sunucuya iletmeden önce IP adresi ve belirlenmiş port numarası ile bağlantı açılarak veri alışverişi başlatılır. Protokol, Open systems Interconnection (OSI) modelinde ulaşım katmanında

uçtan-uca güvenilir bir ortam yaratmayı amaçlar. Ortamın güvenilirliği, kaybolan paketlerin tekrar gönderilmesini temel alır.

Protokolde taşınan veriler 64 KB büyüklüğünü geçmeyecek veri boyutlarına ayırır. Paket içerisine TCP başlıkları eklendikten sonra uygulama katmanına kadar paket taşınır ve veri iletimi gerçekleşir.

TCP protokolünü diğer protokollerden ayıran en büyük özellik kayıt paketler protokol tarafından algılanır ve tekrar gönderimi sağlanır.

Protokol çift yönlüdür (full-duplex). Bu özellik, hem nesnenin veri göndermesini hem de sunucunun veri göndermesine olanak sağlar.

Bazı TCP Soket kullanan bazı uygulamaların port ve işlev bilgisi Tablo 2.1.'de paylaşılmıştır.

Tablo 2.1. TCP Socket Uygulamaları

Port No	**Uygulama / İşlev**
21	File Transfer Protokol (FTP) / Veri Aktarımı
25	Simple Mail Trransfer Protocol (SMTP) / E-Posta
80	Hyper-Text Transfer Protocol (HTTP) / World Wide Web (WWW)

2.2.2. UDP Soket

UDP, nesnelerin veri aktarımında kullandığı protokollerden biridir. Paket içerisinde kaynak port, hedef port, paket uzunluğu ve bütünlük doğrulama kodu eklenerek uygulama modeline kadar paket taşınır.

Protokol çift yönlüdür (full-duplex). Bu özellik, hem nesnenin veri göndermesini hem de sunucunun veri göndermesine olanak sağlar.

TCP protokolü ile olan en büyük farkı bağlantı temelli olmamasıdır. Bağlantı temelli olmaması herhangi bir nesne / uzak sunucu, bağlantıyı dinlemese bile paket gönderimi yapılır.

TCP protokolünün sağladığı kaybolan verileri tekrar iletme yükümlülüğü UDP protokolünde yoktur, bu kontrol mekanizmasının olmaması protokolü TCP protokolüne göre güvensiz fakat veri iletiminde daha hızlı olmasını sağlar.

BÖLÜM 3. METER-BUS PROTOKOLÜ

Günümüzde aldığımız doğalgaz, su, elektrik gibi temel ihtiyaçlarımızın tüketimlerinin hesaplanması için sayaç kullanılmaktadır. Bu sayaçlar, hizmet sağlayıcı firmanın personelleri tarafından sayacın konumuna ulaşıp sayaç üzerindeki değerin göz ile okunması sağlanarak belirli periyotlarda tüketimin ortaya çıkmasında yardımcı rol oynarlar.

Aynı zamanda toplu konutların, sitelerin, alışveriş merkezlerinin artması ile belirli kapasitede metrekare veya kişi olması durumunda payölçer zorunluluğu devlet tarafından getirilmiştir. Bu durumda doğalgaz, su sağlayıcıları tek bir sayaç üzerinden site, alışveriş merkezi gibi konumlarda tek fatura ile hizmet verecek ve bu konumlarda bulunan yönetimler ise çıkacak olan faturaya göre konumda bulunan tüketicilere pay edilmesinde görev alması sağlanmıştır.

Bir site veya alışveriş merkezinde yüzlerce, binlerce daire veya marka olacağını düşünürsek klasik yöntem olarak bilinen göz ile okuma hataya açık ve yasal olmayan bir uygulamadır. Bu hataların ve maliyetlerin önüne geçmek için geliştirilen Meter-Bus (M-Bus), doğalgaz ve su sayaçlarının okunması için Avrupa standardı olan protokoldür. Bu standardizasyon ile sayaç üreticileri donanımlarına haberleşme protokolleri ekleyerek bu protokole uyum sağlamışlardır, bu uyum sayesinde birden fazla marka tek protokolde birleşmesi sayesinde veri iletiminde herhangi bir problem olmayacaktır. Bu protokol kablolu ve kablosuz (Wireless M-Bus) olarak iki grupta toplanmıştır.

M-Bus protokolü geliştirilirken çok sayıda sayacın bağlanabilir olması, ağ genişletme imkanı sunması, sayaç arızalarını raporlayabilme, düşük güç tüketimli olması, kabul edilebilir veri iletimi hızının olması esas alınmıştır.

3.1. M-Bus İletişim

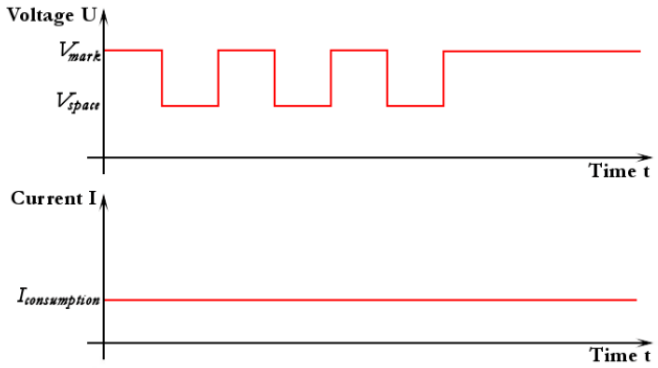
M-Bus iletişimi temelde Universal Asynchronous Receiver / Transmitter (UART) arayüzü kullanır. Bu arayüz, Start Bit (Başlangıç Biti), Parity (Tek / Çift), Baud Rate (Baud Hızı) ve Stop Bit (Durdurma Biti) gibi bilgilere ihtiyaç duymaktadır. Baud hızı her ne kadar 300 ile 38,400 Baud arası kullanılmaya müsait olsada 9600 Baud üzeri hem yaygın olarak kullanılmaz hem de fiziksel katman bu hıza müsait olmayabilir. M-Bus harici bir kablo ile çevrim döngüsü (clock-cycle) sağlamaz kendi içerisinde bu mekanizma mevcuttur. Kablo sayısını azaltmak ve ortak veri yolunda collision (çakışma) olmaması için master-slave (ana-ek) veri iletim yöntemine sahiptir. Bu sayede iletişimde aynı anda hem gönderme hem de alma işlemleri tek çiftli kablo (single pair) kablo ile yapılmaktadır. Haberleşme işlevinin dışında master (okuyucu), her bir slave (sayaç) için güç kaynağı sağlar. Sağladığı güç ile hat üzerinde gerilim değişimleri oluşabilir. Bu gerilim değişimi standartta açıkça belirtilmediği için 24 V ile 50 V arasında değişkenlik gösterir.

M-Bus üzerinde okuyucudan sayaca iletişim (Master to Slave – M2S) ve sayaçtan okuyucuya iletişim (Slave to Master – S2M) olmak üzere iki türe ayrılır.

Pilot Elektronik firmasının üretmiş olduğu PMM-10 USB – MBus dönüştürücüsü kullanılarak sayaç ile M-Bus protokolü ile iletişim sağlanmıştır. Bu ürün M-Bus hattında 10 adet sayaç ile haberleşebilecek akım sağlayabilmektedir.

3.1.1. Master to Slave (M2S) İletişim

Okuyucu ile sayaç kendi arasında talep-cevap (request - response) yöntemi ile iletişim sağlar. M2S iletişimde sayaç değerlerini, konfigürasyon ayarlarını değiştirme gibi talepler yapılabilir. Lojik değer olarak 1 sabit Vmark gerilimi temsil etmekte, lojik 0 değeri ise -12V değişken gerilimi temsil etmektedir [6]. Bu nedenle iletişim yaklaşık 12 V gerilim değişimi ile tanımlanır aynı zamanda iletim sırasında tüketim akımı sabittir. İletişim sırasındaki gerilim ve akım grafikleri Şekil 3.1'de gösterilmiştir [6].

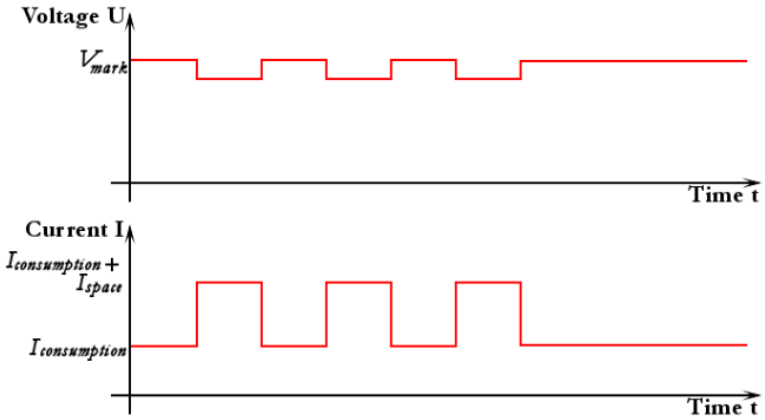


Şekil 3.1. M-Bus M2S İletişimi Sırasında Gerilim ve Akım Grafiği

3.1.2. Slave to Master (S2M) İletişim

Sayaçlar iletişim için akım tüketimlerini kendisi modüle eder. Bu durumda akım M2S iletişimde olduğu gibi sabit kalmayacak, okuyucu ünite tarafından sağlanan güç ile ihtiyacı akımı çekecektir.

İletişim olmadığı durumda (idle) sayaçların akım tüketimleri sabittir bu değer yaklaşık 1,5 mA değerindedir [6]. Bu sabit akım protokol dökümanında birim yük veya Imark olarak tanımlanır. Sayacın akım tüketimi birim yükün tam katları olmaktadır. Örneğin sayaç 5 mA akım ihtiyacı ile okuyucudan güç çekmek isterse M-Bus hattı üzerinden 6 mA akım yani 4 birim yük iletecektir. Okuyucu üniteler maksimum 250 birim yük sağlayabilir. Sayaçtan okuyucu yönüne olan iletişimin gerilim ve akım grafikleri Şekil 3.2'de gösterilmiştir [6].



Şekil 3.2. M-Bus S2M İletişimi Sırasında Gerilim ve Akım Grafiği

BÖLÜM 4. RASPBERRY-PI

Raspberry Pi'nin tarihi 2006 yılında tanıtılan ana konsepti, özellikle eğitim amaçlı kullanım için tasarlanmış ve Python programlama diline yönelik kullanılan ATmega644'e dayanmaktadır. Raspberry Pi, İngiltre'de Raspberry Pi adlı bir kuruluş tarafından geliştirilen, kredi kartı boyutunda olan tek kartlı bilgisayardır (single board computer). Bu vakfın birincil amacı, eğitim kurumlarında ve gelişmekte olan ülkelerde temel bilgisayar bilimlerinin öğrenilmesine destek olmaktır. Raspberry Pi'nin ilk nesli 2012 yılında A ve B modelleri olmak üzere piyasaya sürülmüştür. Günümüzde dördüncü nesil bilgisayarları ile hayatımızda olan Raspberry Pi, 2021 yılında Raspberry Pi Pico adında C / C++ ve MicroPython dillerini derleyip çalıştırabilen ürününü tanıtmıştır.

Fiyat avantajı ile akademik çalışmalarda, IoT projelerinde aktif olarak kullanılan hazır donanımdır. Raspberry Pi Pico haricinde diğer Raspberry Pi donanımları içerisinde günümüzde kullanılan 3. parti Linux dağıtımları (LibreElec, Ubuntu Desktop, Ubuntu Core, Ubuntu Server, TLXOS) ve Raspberry Pi için özel geliştirilen Linux dağıtımı Raspberry Pi OS işletim sistemleri çalıştırılabilmektedir. Uzak (Bulut) sunucularda çalışan veritabanı uygulamaları (MySQL, NoSQL), haberleşme uygulamaları (MQTT, REST) veya geliştirici olarak geliştirebileceğiniz Java, .NET Core, C/C++, Python gibi uygulamalar Raspberyy Pi üzerinde de çalıştırılabilir.

Raspberry Pi ile çalışan uygulamalar uzak sunucu ile birleştirildiğinde yapılabilecek IoT çalışmaların sınırı olmamaktadır. Örneğin ilk bulut haberleşme özellikli espresso makinesi Raspberry Pi ile yapılmıştır. Ev ve giyim mağazaları için akıllı ayna, seralar için akıllı sulama sistemleri, akıllı ev sistemleri, ısıtma & soğutma sistemlerinin kontrolü, hava kalitesi ölçümleme istasyonu, kablosuz ev zili, akıllı asistan, bebek kamera takibi gibi bir çok uygulama Raspberry Pi ile çalıştırılabilir.

Buna benzer bir projeyi de Raspberry Pi vakfı 2020 yılında hayata geçirip Raspberry Pi 400 adında bir ürün tanıtmıştır. Klavye içersine konulmuş Raspberry Pi donanımı ve bir fare ile satılmakta olan Raspberry Pi 400, donanımın üzerinde bulunan HDMI çıkışı ile monitöre bağlandığında kullanıma hazır bir Linux dağıtımı ile bilgisayar kullanmaya hemen başlama imkanı sağlamaktadır.

Geniş kullanım alanı sunan Raspberry Pi kullanıcıları gün geçtikçe artmakta ve bu kullanıcıların desteklediği / yayınladığı açık kaynak uygulamalar topluluğa büyük katkı sağlamaktadır. Bu çalışmada Şekil 4.1'de gösterilen Raspberry Pi 4 donanımı kullanılacaktır.



Şekil 4.1. Raspberry Pi 4

4.1. Raspberry Pi Donanım Özellikleri

Her nesilde sağladığı bellek, hafıza, bağlantı arayüzü seçenekleri ile farklılıkları olan Raspberry Pi'nin donanım özellikleri Tablo 4.1'de gösterilmiştir.

Tablo 4.1. Raspberry Pi Donanım Özellikleri

Nesil	Model	Bellek	Bağlantı	Çıkış Tarihi
Raspberry Pi 1	A, B	256 MB	Ethernet	2012
	A+, B+	512 MB		2014
Raspberry Pi 2	B	1 GB	Ethernet	2015
Raspberry Pi Zero	Zero	512 MB	-	2015
	W/WH		Wi-Fi	2017
Raspberry Pi 3	A+	512 MB	Ethernet & Wi-Fi	2018
	B	1 GB		2016
	B+			2018
Raspberry Pi 4	B	1, 2, 4, 8 GB	Ethernet & Wi-Fi	2019
	400	4 GB		2020
Raspberry Pi Pico	-	264 KB	-	2021

BÖLÜM 5. YÖNTEM

Bu bölümde uçtan uca NB-IoT sayaç okuma uygulaması geliştirilmiş olup, bu uygulamaya ait veri güvenliğini iyileştirmek için yapılan çalışmalar raporlanmıştır.

Bu çalışma kapsamında veri olarak adlandırılan 2 adet veri bulunmaktadır. Bunlar, sayaç verisi ve kullanıcı verisidir. Sayaç verisi, Raspberry Pi tarafından gönderilen sayacın seri numarası ve sayaç değerlerini içermektedir. Kullanıcı verisi ise sisteme önceden tanımlanmış abone bilgilerini içermektedir.

Uygulama Raspberry Pi içerisinde çalışan Java uygulamasının okuyucu ünite ile haberleşip sayaçtan verileri alıp Quectel BC96 NB-IoT geliştirme kiti ile uzak sunucuya iletmesi ile başlamakta, uzak sunucuya iletilen veriler sayacın hangi aboneye ait olduğuna bakmadan kayıtları veritabanına kaydetmektedir. Son tüketicilerin sahip olduğu mobil uygulama aracılığı ile kişiler sayaç verilerini görüntülemektedir.

Sayaç verisinin güvenliği uzak sunucuya gönderilmesi ile başlamaktadır. Uzak sunucuya veri gönderilirken uzak sunucu, istemcilerden bir anahtar değer istemektedir bu anahtar değer Raspberry Pi uygulaması içerisinde gömülüdür aynı zamanda uzak sunucuya eklenen Secure Sockets Layer (SSL) sertifikası ile Raspberry Pi'nin gönderdiği anahtar değer başka istemciler tarafından izlenmemesi sağlanmıştır. Bu sayaç verisi sunucuya iletilirken güvenliği sağlanmıştır.

Kişisel verilerin güvenliği ise uzak sunucuda veritabanında saklanmaktadır. Burada uluslararası belirlenmiş standartlar irdelenmiş olup, alternatif olabilecek çözümler sunulmuştur.

5.1. M-Bus Destekli Sayaçlar

Çalışmada 1 adet kalorimetre, 1 adet soğuk su ve 1 adet sıcak su sayacı kullanılmıştır.Uygulamada farklı sayaçların aynı M-Bus protokolü ile çalıştırılması amaçlanmış olup uygulamanın kullanım alanında esneklik sağlanmıştır.

Sayaçların M-Bus protokolü ile okunması için ihtiyaç duyulan sayaç seri numarası bilgisi sayaç üzerinde Şekil 5.1'de işaretlenmiş alanlardan alınıp veritabanına kayıt edilmesi sağlanmıştır.



Şekil 5.1. M-Bus Sayaç Seri No Bilgisi

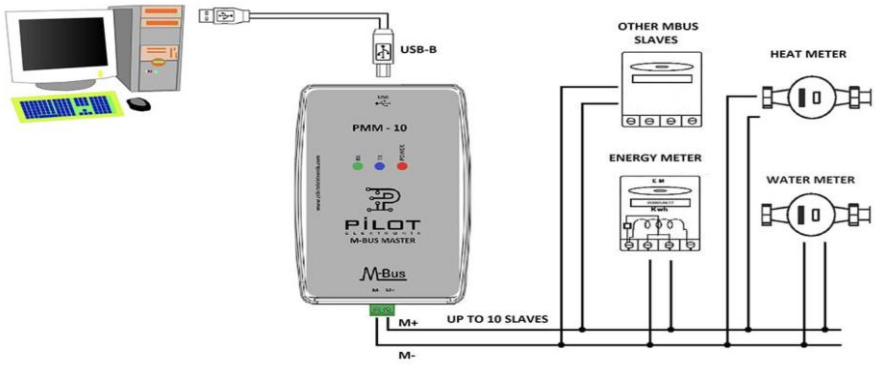
5.2. mBus - USB Dönüştürücü Donanımı

Çalışmada sayaçların okunması için gerekli olan master (okuyucu) cihaz Pilot Elektronik firması tarafından üretilen PMM-10 donanımı ile yapılacaktır. PMM-10'a ait teknik veriler Tablo 5.1'de gösterilmiştir.

Tablo 5.1. PMM-10 Donanım Özellikleri [7]

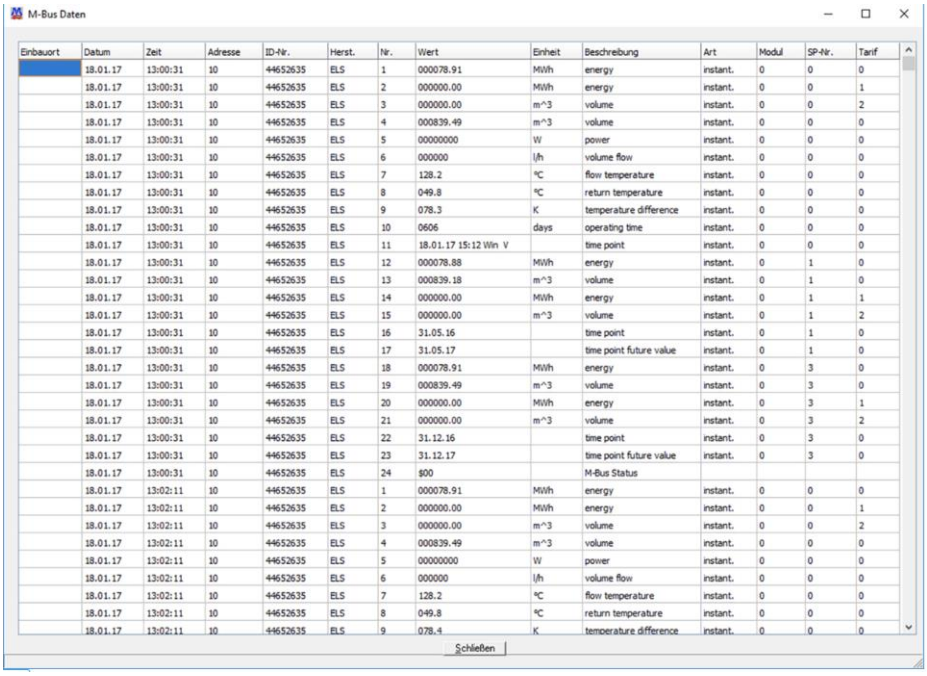
Özellik	Özellik Değeri
Giriş Gerilimi	5 VDC
Maksimum Güç Tüketimi	2.5 W
M-Bus Hat Gerilimi	36 VDC
En Fazla M-Bus Slave (Sayaç) Sayısı	10 Adet
Bağlantı Arayüzü	USB

PMM-10'a ait bağlantı şeması Şekil 5.2.'de gösterilmiştir. Çalışma sırasında şemada gösterilen bilgisayar yerine Raspberry Pi kullanılmıştır.



Şekil 5.2. PMM-10 Bağlantı Şeması [7]

USB Arayüzü üzerinden açılan seri port bağlantısı 2400 baud, parite bilgisi çift, başlangıç biti 0, durdurma biti 1 olacak şekilde MBSheet yazılımı üzerinden donanımın çalışırlığı test edilmiştir. Sayacın M-Bus protokolü üzerinden MBSheet yazılımına ilettiği bilgiler Şekil 5.3'de gösterilmiştir.


M-Bus Daten

Einbauort	Datum	Zeit	Adresse	ID-Nr.	Herst.	Nr.	Wert	Einheit	Beschreibung	Art	Modul	SP-Nr.	Tarif
	18.01.17	13:00:31	10	44652635	ELS	1	000078.91	MWh	energy	instant.	0	0	0
	18.01.17	13:00:31	10	44652635	ELS	2	000000.00	MWh	energy	instant.	0	0	1
	18.01.17	13:00:31	10	44652635	ELS	3	000000.00	m^3	volume	instant.	0	0	2
	18.01.17	13:00:31	10	44652635	ELS	4	000839.49	m^3	volume	instant.	0	0	0
	18.01.17	13:00:31	10	44652635	ELS	5	00000000	W	power	instant.	0	0	0
	18.01.17	13:00:31	10	44652635	ELS	6	000000	l/h	volume flow	instant.	0	0	0
	18.01.17	13:00:31	10	44652635	ELS	7	128.2	°C	flow temperature	instant.	0	0	0
	18.01.17	13:00:31	10	44652635	ELS	8	049.8	°C	return temperature	instant.	0	0	0
	18.01.17	13:00:31	10	44652635	ELS	9	078.3	K	temperature difference	instant.	0	0	0
	18.01.17	13:00:31	10	44652635	ELS	10	0606	days	operating time	instant.	0	0	0
	18.01.17	13:00:31	10	44652635	ELS	11	18.01.17 15:12 Win V		time point	instant.	0	0	0
	18.01.17	13:00:31	10	44652635	ELS	12	000078.88	MWh	energy	instant.	0	1	0
	18.01.17	13:00:31	10	44652635	ELS	13	000839.18	m^3	volume	instant.	0	1	0
	18.01.17	13:00:31	10	44652635	ELS	14	000000.00	MWh	energy	instant.	0	1	1
	18.01.17	13:00:31	10	44652635	ELS	15	000000.00	m^3	volume	instant.	0	1	2
	18.01.17	13:00:31	10	44652635	ELS	16	31.05.16		time point	instant.	0	1	0
	18.01.17	13:00:31	10	44652635	ELS	17	31.05.17		time point future value	instant.	0	1	0
	18.01.17	13:00:31	10	44652635	ELS	18	000078.91	MWh	energy	instant.	0	3	0
	18.01.17	13:00:31	10	44652635	ELS	19	000839.49	m^3	volume	instant.	0	3	0
	18.01.17	13:00:31	10	44652635	ELS	20	000000.00	MWh	energy	instant.	0	3	1
	18.01.17	13:00:31	10	44652635	ELS	21	000000.00	m^3	volume	instant.	0	3	2
	18.01.17	13:00:31	10	44652635	ELS	22	31.12.16		time point	instant.	0	3	0
	18.01.17	13:00:31	10	44652635	ELS	23	31.12.17		time point future value	instant.	0	3	0
	18.01.17	13:00:31	10	44652635	ELS	24	$00		M-Bus Status				
	18.01.17	13:02:11	10	44652635	ELS	1	000078.91	MWh	energy	instant.	0	0	0
	18.01.17	13:02:11	10	44652635	ELS	2	000000.00	MWh	energy	instant.	0	0	1
	18.01.17	13:02:11	10	44652635	ELS	3	000000.00	m^3	volume	instant.	0	0	2
	18.01.17	13:02:11	10	44652635	ELS	4	000839.49	m^3	volume	instant.	0	0	0
	18.01.17	13:02:11	10	44652635	ELS	5	00000000	W	power	instant.	0	0	0
	18.01.17	13:02:11	10	44652635	ELS	6	000000	l/h	volume flow	instant.	0	0	0
	18.01.17	13:02:11	10	44652635	ELS	7	128.2	°C	flow temperature	instant.	0	0	0
	18.01.17	13:02:11	10	44652635	ELS	8	049.8	°C	return temperature	instant.	0	0	0
	18.01.17	13:02:11	10	44652635	ELS	9	078.4	K	temperature difference	instant.	0	0	0

Schließen

Şekil 5.3. MBSheet Uygulaması ile Sayaç Değerleri Görüntülenmesi

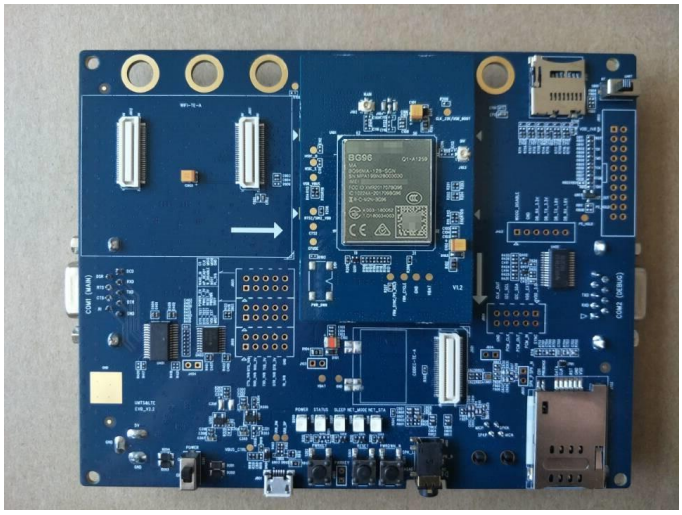
Bu doğrulama ile PMM-10, USB üzerinden Raspberry Pi'ye bağlanarak sayaç okuma işlemini uygulamaya dahil edilmiştir.

5.3. Quectel BC96 NB-IoT Geliştirme Kiti

Raspberry Pi donanımının internet erişimi için kullanılan Quectel firmasının üretmiş olduğu BG96 modülünün temel alındığı geliştirme kiti kullanılmıştır. Modül, son kullanıcıya sağladığı birden fazla hücresel seçenekleri ve Türkiye'de ulaşılabilir olması nedeniyle tercih edilmiştir.

BG96 modülü diğer Quectel ürünleri gibi Hayet Komut Seti diğer adı ile AT komut setini kullanmaktadır. Bu komut setleri kullanılarak, modül üzerinde internet erişimi ayarları, sms gönderme, sesli arama yapma gibi bir çok özelliği bu komutlar aracılığı ile yapmaktadır. AT komut setinin tamamı Quectel BG96 referans at komut seti dökümanında paylaşılmıştır [8].

Çalışma içerisinde Turkcell operatörüne ait NB-IoT sim kartı kullanılmıştır. Çalışma yapıldığı sırada Turkcell sadece kurumsal müşterilerine bu hizmeti sağlamakta ve belirli kapsama alanında bu hizmeti sağlamaktadır [9].



Şekil 5.4. Quectel BG96 Geliştirme Kiti

5.4. Raspberry Pi - Sayaç Okuma Uygulaması

Çalışmada sayaç verisi olarak adlandırılan verinin elde edilmesi için Raspberry Pi üzerinde çalışan Java uygulaması geliştirilmiştir.

Java uygulaması ilk önce uzak sunucudan Raspberry Pi'ye ait seri numarasına göre veritabanından okuma periyodunu almaktadır. Periyot bilgisi ile çalışacak iş planlanır, zamanı geldiğinde Raspberry Pi uzak sunucudan sayaç listesini alır ve okuyucu aracılığı ile okumaya başlar. Şekil 5.5'de planlanma ve çalıştırma fonksiyonları gösterilmiştir.



Şekil 5.5. Java Uygulaması Okuyucu Planlama ve Çalıştırma Fonksiyonları

Zamanı geldiğinde, herhangi bir sayaç listesi bulunmaz ise "Sayaç Listesi Boş" olarak, sayaç listesinin dolu olması ve sayaç üzerinden veri alınmaması durumunda kayıtlara "Telemetri listesi boş" olarak, sayaç üzerinden veri alınması durumunda ise verileri uzak sunucuya gönderip "X (adet) Telemetriler başarıyla gönderildi " mesajları kayıt edilir.

Sayaç okuma sırasında, Raspberry Pi USB aracılığıyla okuyucu ile seri port haberleşerek 2400 baud hızında sayaç okuma işlemi için talep yapar ve cevapları alır.

Alınan veriler REST API kullanılarak, uzak sunucuya POST methodu ile gönderimi sağlanır.

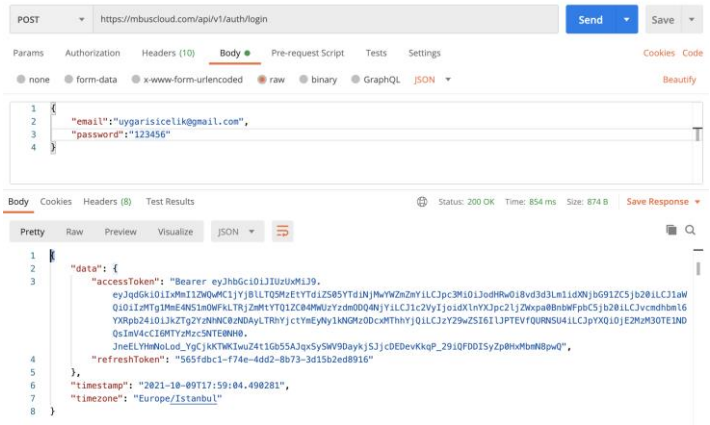
5.5. iOS Mobil Uygulama – Sayaç Verileri İzleme Uygulaması

Veri güvenliğinin sağlandığı diğer nokta ise kullanıcı tarafında yetkisiz erişimlerin kısıtlandığı iOS mobil uygulamasıdır.

Mobil uygulama Swift dilinde yazılmış olup, tüm sunucu isteklerinde Alamofire kütüphanesi kullanılmıştır [10]. Kullanıcı arayüz katmanı ise Apple'ın sağlamış olduğu UIKit komponentleri kullanılmıştır.

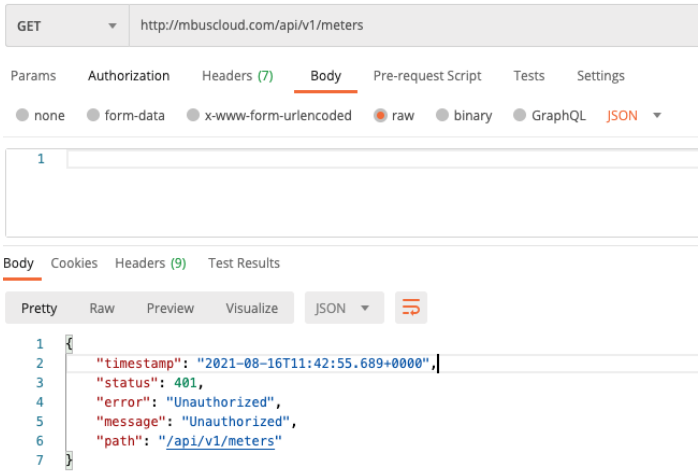
Çalışmada ana amaç veri güvenliği olması nedeniyle mobil uygulama tamamlayıcı yazılım ürünü olarak geliştirilmiştir, bu nedenle uygulama üzerinde herhangi bir kullanıcı arayüzü veya kullanıcı deneyimi çalışması yapılmamıştır.

iOS uygulamasında her kullanıcı mail adresi ve şifresi ile giriş yapar ve uzak sunucu elindeki son verileri son kullanıcıya REST API üzerinden GET methodu ile verir. Bu methodun uzak sunucuda bazı gereksinimleri bulunmaktadır, giriş yapıldıktan sonra sunucu tarafından son kullanıcıya arka planda verilen anahtar ile diğer istekler kabul edilmektedir, aksi takdirde uzak sunucu yetkisiz erişim olduğunu bilip kullanıcının taleplerini reddedecektir. Başarılı giriş sonucunda elde edilen anahtar değer accessToken olarak adlandırılmıştır ve Şekil 5.6'da giriş isteğinin örneği gösterilmiştir. Bu adımdan sonra yapılacak olan bütün istekler bu accessToken ile birlikte yapılması gerekecektir.



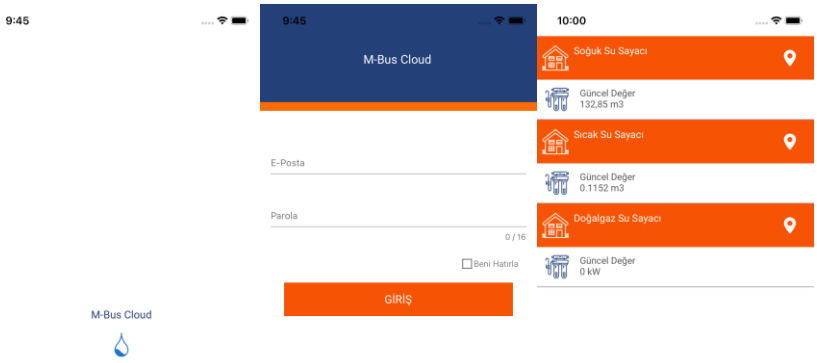
Şekil 5.6. Giriş İstek Örneği ve accessToken Değeri

Anahtar değer olmadan yapılan bütün istekler unauthorized yani yetkisiz işlem olarak adlandırılıp veri güvenliği sağlanmıştır. Yetkisiz isteğe örnek Şekil 5.7'da gösterilmiştir.



Şekil 5.7. Yetkisiz İstek Talebi

Aynı zamanda uygulamaya ait giriş ve sayaç verilerinin bulunduğu ekran görüntüleri Şekil 5.8'de paylaşılmıştır.



Şekil 5.8. iOS Uygulama Ekran Görüntüleri

Uygulamanın giriş ekranında ve sayaç değerlerinin uzak sunucudan alınmasında görevli fonksiyonlar Şekil 5.9'da paylaşılmıştır, sayaç değerlerinin alınması isteğinde görülen Authorization parametresi, giriş yapıldıktan sonra uzak sunucunun iletmiş olduğu anahtar değer bilgisidir.



```
public func login<T:Decodable>(username: String, password: String, completion: @escaping (Result<ApiResponse<T>>) -> Void) {
        Alamofire.request(Parameters.REST.SERVICE_URL + Parameters.REST.EndPoint.LOGIN,method: .post, parameters: ["email":username,"password":password], encoding:
JSONEncoding.default, headers: ["Platform":"MOBILE"]).response {
            response in
            do {
                completion(.success(try JSONDecoder().decode(ApiResponse<T>.self,from: response.data!)))
            }
            catch(let error) {
                print(error.localizedDescription)
                completion(.failure(error))
            }
        }
}

public func getMeterValues<T:Decodable>(completion: @escaping (Result<T>) -> Void) {
        Alamofire.request(Parameters.REST.DEVICE_SERVICE_URL + "/meters", method: .get, parameters: ["Authorization" :  (self.authToken?.accessToken)! ).response {
            response in
            do {
                if(response.response?.statusCode == 200) {
                    print(String(data: response.data!, encoding: .utf8))
                    completion(.success(try JSONDecoder().decode(T.self,from: response.data!)))
                } else {
                    completion(.failure("" as! Error))
                }
            }
            catch(let error) {
                print(error.localizedDescription)
                completion(.failure(error))
            }
        }
}
```

Şekil 5.9. Giriş ve Sayaç Değerlerinin Fonksiyonları

5.6. Uzak Sunucu Bileşenleri

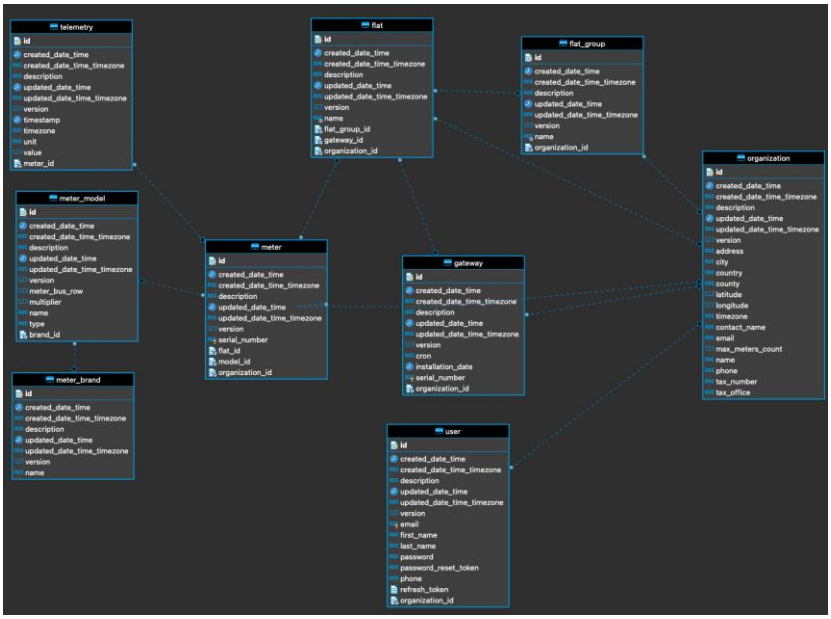
Bu bölümde Nesnelerin İnterneti uygulamasında “internet” kavramının olması için ihtiyacımız olan veritabanı, arka-uç uygulaması ve bileşenleri incelenmiştir.

5.5.1. Veritabanı

Veritabanı, sayaç verilerinin ve kullanıcı verilerinin saklanması, arka uç uygulaması tarafından tekrar okunup istemcilere iletmesi için kullanılan bileşendir. Çalışmada MySQL ilişkisel veritabanı kullanılmış olup, mbuscloud adında veritabanı oluşturulmuştur. Çalışma içerisinde 3 sayaç kullanılsada veritabanı mimarisi birden fazla konumda, birden fazla sayaç ve son kullanıcısı olacak bir mimariye göre tasarlanmıştır.

Tasarlanan veritabanı modellemesine ait ilişkisel diyagram Şekil 5.10’da gösterilmiştir.

Verilerin güvenliğinin en üst düzeyde olması gereken bu bileşende veritabanına sadece arka uç uygulamasının çalıştığı sunucunun IP adresi tanımlanmıştır. Çalışma sırasında tek sunucu üzerinde kurulu olması nedeniyle sadece 127.0.0.1 IP adresi (yerel makina) tanımlanmıştır. Bu sayede yetkisiz kişilerin veritabanı üzerinden açılan portlara erişimi olmayacak ve bir güvenlik katmanı eklenmiş olacaktır.



Şekil 5.10. Veritabanı İlişkisel Diagramı

5.5.2. Arka Uç Uygulaması

Raspberry Pi, iOS mobil uygulama ve veritabanı gibi bileşenlere veri alışverişi yapan ana bileşendir.

Çalışmada Raspberry Pi ile olan veri alışverişi veritabanında bulunan gateway tablosu ile başlamaktadır. Arka uç uygulaması Şekil 5.11'da belirtilen fonksiyon ile Raspberry Pi'a ait olan zaman periyodunu alıp Raspberry Pi'ye iletmekle yükümlüdür.



Şekil 5.11. Raspberry Pi Periyot Fonksiyonları

Raspberry Pi'ye sağladığı diğer servis ise sayaç sayaç bilgileri NB-IoT modül tarafından iletilmesi için telemetri servisi ve veritabanına kayıt katmanıdır. Bu katmana ait fonksiyon da Şekil 5.12'de gösterilmiştir.



Şekil 5.12. Telemetri Servisi ve Veritabanı Kayıt Fonksiyonu

Mobil uygulama için kullanıcılara sağlanan iki servis bulunmaktadır. Bunlardan ilki kullanıcının sisteme giriş yapması için gereken servistir. İkincisi ise kullanıcıya ait olan sayaçların son değerleri ile ileten servistir.

Arka uç uygulamasının veritabanı işlemleri için nesne-ilişkisel eşleme, yazma, okuma, güncelleme gibi işlemler için Java dili için geliştirilmiş Hibernate yapısı kullanılmıştır.

5.7. Veri Güvenliği Kapsamında Yapılan Çalışmalar

Çalışmanın temel konusu olan veri güvenliği için yapılan geliştirmeler ve servis tasarımları bu alt bölümde anlatılmaktadır.

Çalışmada sayaç verisi (telemetri) ve kişisel veri olmak üzere iki çeşit veri tipi bulunmaktadır. İki veri türü içinde farklı güvenlik adımları geliştirilmiş ve aynı zamanda sunucu tarafında da ekstra güvenlik sertifikaları eklenmiştir.

Raspberry Pi tarafından elde edilen veriler Quectel BC96 geliştirme kitine iletilen AT komutu ile tarafından uzak sunucuya iletilir. Bu adımda yetkisiz kişilerin uzak sunucuya Raspberry Pi gibi davranıp veri göndermesi engellenmesi gerekmektedir. Bu durumda veri toplamakla yükümlü her bir Raspberry Pi'nin seri numarası ile veriyi iletmesi bir güvenlik katmanı olarak eklenmesi bir güvenlik adımı olabilirdi fakat sahada kullanım açısından herkesin erişiminin olabileceği bir yerde olması düşünüldüğünde seri numarasını geliştirilen uygulamanın içerisine yerleştirildiğinde uygulama tersine mühendislik ile açıldığında tüm iletişim çözülebilir olmaktadır. Bu nedenle seri numarasını uygulama katmanında tutmak yerine işletim sistemi katmanında çevresel değişkenler alanında tutmak, çalışmada sayaç verisini daha güvenli hale getirmiştir.

Çalışmada, kişisel verilerin (Abone bilgileri, isim soyisim, sayaç-abone eşletirilmesi, daire) gibi verilerin güvenliğinin sağlanması veritabanı güvenliğinin sağlanmasından geçmektedir. Bu güvenliğin sağlanması için veritabanın bulunduğu sunucuda arka uç uygulaması da çalıştırılmıştır. Veritabanı konfigürasyonunda uzak erişime tamamen kapatılması ve sadece yerel makine üzerinden (127.0.0.1) erişimi sağlanmıştır bu sayede sadece arka uç uygulaması veritabanına erişebilecek, uzaktan erişim sadece sunucuya ait root (ana kullanıcı) aracılığı ile yapılmakta olacaktır.

Çalışmanın Raspberry – Pi ve iOS mobil uygulama katmanlarına hizmet veren sunucuya SSL sertifikası kurulmuştur. Bu sertifika ile WireShark, tcpdump gibi programlar ile başka kişilerin ağ trafiğini izlemesinin önüne geçilmiştir. Raspberry Pi veya iOS mobil uygulamaya servis edilen anahtar değerlerin güvenliği sağlanmıştır.

Yapılan bu çalışmalar literatürde bulunan farklı atak yöntemlerine karşı geliştirilmiş olup, aşağıdaki atak çeşitlerinde etkisi gözlemlenmiştir.

5.8. Atak Yöntemleri

5.8.1. Man in the Middle (MitM) Saldırısı

MitM, Kötü niyetli bir kişinin iki IoT iletişim cihazı arasındaki ağ içerisinde olduğu veri saldırısının gelişmiş bir sürümüdür. Atağı yapan kişi, her iki uç noktanın kimliğini manipüle eder ve iletişim trafiğini kesmek için her bir hedefle bağımsız bağlantılar kurar ve ardından bunlar arasında iletileri aktarır ve iletir. Bu şekilde kişi, paketleri geciktirme, klonlama, yeniden oynatma, yanıltma veya düşürme yeteneğine sahiptir. Bu manipülasyon, tüm konuşma saldırgan tarafından kontrol edilirken uç noktaları doğrudan birbirleriyle konuştuklarına inandırır. Hassas sağlık durumu, endüstriyel IoT kontrol geri bildirimi ve hatta ev kapılarının gizli anahtarları gibi güvenilir bilgiler, MitM'li bir saldırgan tarafından sahte olabilir ve değiştirilebilir, böylece ciddi IoT güvenlik sorunlarına neden olabilir [4].

Bu saldırıya önlem olarak çalışma içerisinde sunucuya eklenen SSL sertifikası ve iOS mobil uygulama üzerinde JSON Web Token (JWT) doğrulama yöntemleri eklenerek olası MitM saldırılarının önüne geçilmesi amaçlanmıştır.

5.8.2. Denial-of-Service (DoS) Saldırısı

DoS saldırısı, en yaygın ağ saldırılarından biridir ve IoT sistemlerine karşı çarpıcı bir etkiye sahip olabilir. İstemcilere hizmet vermekle yükümlü olan sunucular, gelen tüm isteklere cevap vermekle yükümlüdürler. DoS saldırısındaki amaç, sunuculara sürekli istek yapılarak sunucuların farklı kişilere cevap vermesini güçleştirmektir. Saniyede 100 isteğe cevap verebilen bir sunucuya saniyede 500 istek iletilerek sunucunun hizmet vermesini engellemektir. Distributed DoS (DDoS) atağında ise birden fazla istemci aynı saldırıyı yaparak isteklerin engellenmesini zorlaştırmayı amaçlamaktadır [4].

Bu saldırıya önlem olarak uzak sunucu üzerinde ek güvenlik duvarı ve alternatif olarak DigitalOcean firmasının sağlamış güvenlik hizmetleri kullanılabilir.

5.8.3. Replication Saldırısı

Replication saldırısı, IoT sistemlerde yoğun olarak kullanılan saldırı türüdür. Bu saldırı türünde nesnelerin ürettiği verilerin sunucuya gönderilmesi sırasında mesaj yapısını öğrenilmesi ve verilerin değiştirilerek manipüle edilmesi hedeflenmektedir. Bu

atak türünde veri ele geçirilmesi yerine nesnelerin ürettiği verilerin değiştirilmesi beklenmektedir [11].

Cihaz manipülasyonunun önüne geçmek amacıyla uzak sunucu ve nesne arasında SSL iletişim kurulması ve ek önlem olarak her cihazın sahip olduğu seri numarası ile iletişim kurulması tasarlanmıştır.

BÖLÜM 6. BULGULAR VE YORUMLAR

Bu bölüm içerisinde, Yöntem bölümünde bahsedilmiş uçtan uca tasarlanan NB-IoT uygulamasında veri güvenliğinde alınan önlemler ve sistemin genel çalışma prensibi ve akışından bahsedilmiştir. Aynı zamanda yine bu bölüm içerisinde ortaya çıkan güvenlik problemlerine hangi çözümler sağlandığından da bahsedilmiştir.

6.1. Sisteme Genel Bakış

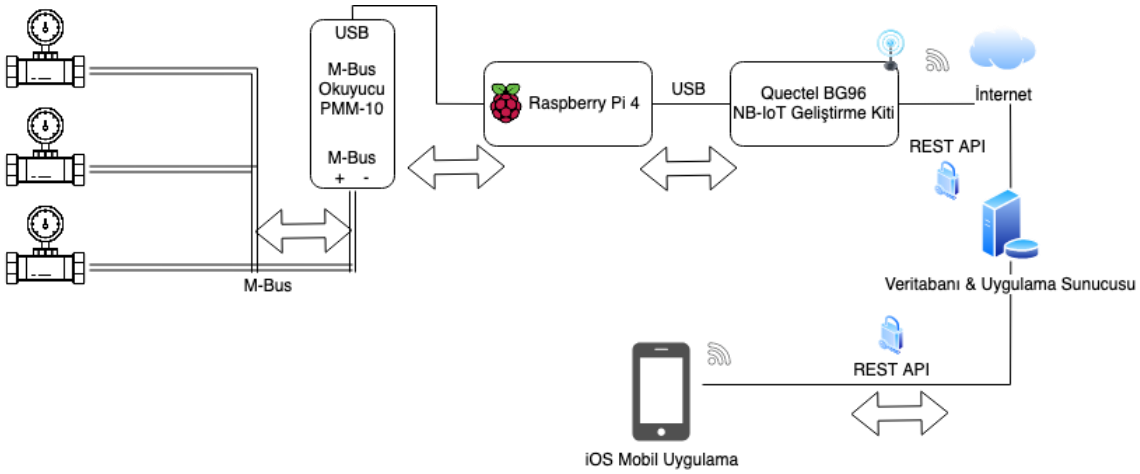
Tedarik edilen 3 adet farklı marka ve farklı özelliklerde olan 3 adet sayacın, M-Bus hatları okuyucu donanıma bağlanarak Raspberry Pi tarafından okunulması sistemin ilk adımıdır. Raspberry Pi Uzak sunucudan okuma periyodu bilgisini almak için AT komutları aracılığı ile Quectel BG96 geliştirme kiti aracılığı ile uzak sunucudan konfigürasyon bilgilerini istemektedir. Konfigurasyon bilgilerinin gelmesi ile belirlenen periyot için okuma işi planlanır ve sayaç okuması sağlanır.

Okunan sayaç değeri internet ortamına geliştirme kiti aracılığı ile uzak sunucuya iletilmiştir. Veri gönderimini sağlayan servis geliştirmesi tamamlanması ile veri gönderimi sırasında verinin manipüle edilebilir olduğu farkedilmiştir. Aynı servisi kullanan başka istemcilerin kullanması durumunda arka uç uygulamasının bunu kabul ettiği ve veritabanına kaydettiği gözlemlenmiştir. Bu adımda Raspberry Pi ünitelere seri numarası ve sunucuya SSL sertifikası kurulmuştur. Okunan verilerin uzak sunucuya gönderilmesi ile uzak sunucu tarafında Raspberry Pi'ye ait seri numarası doğrulanıp veritabanına kaydedilmesi sağlanmıştır.

Gönderilen verilerin, son tüketiciler tarafından görüntülenmesi için geliştirilen mobil uygulama iOS ortamında Swift yazılım dili ile geliştirilmiştir. Uygulamaya elektronik posta adresi ve şifre ile giriş yapılması bu girişin doğrulanması sonucunda kişiye Json Web Token(JWT Token) verilmesi sağlanmıştır. Giriş adımından sonra uzak sunucu ile yapılacak tüm işlemler bu anahtar aracılığı ile iletişim kurulması sağlanmıştır. Sunucuda SSL sertifikası olması bu anahtar değerinin ele geçirilmesini zorlaştırmaktadır.

Aynı zamanda anahtar değerin olmaması veya hatalı olması durumunda yetkisiz kişiler tüketicinin sayaç verisini görmesini imkansız kılacaktır.

Çalışmanın genel akışı Şekil 6.1'de gösterilmiştir.



Şekil 6.1. Sistemin Genel Akışı

BÖLÜM 7. SONUÇLAR

Nesnelerin İnterneti uygulamaları gün geçtikçe hayatımızda daha fazla yer etmekte. Artan uygulamalar ve donanımlar uçtan uca çözümler hayatımızı kolaylaştırsada verilerimizi paylaşmamız hem dijital hem fiziksel güvenliğimizi risk altına almaktadır. Bu çalışma kapsamında olabilecek sızma / manipüle senaryoları düşünülüp uçtan uca NB-IoT uygulaması geliştirilmiştir.

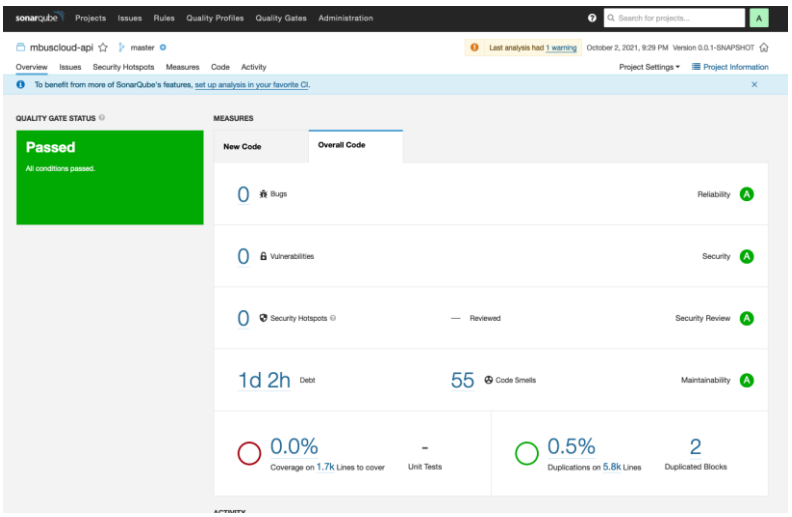
Bu çalışmayı standart Wi-Fi, Ethernet gibi internet arayüzleri ile yapmak yerine NB-IoT gibi güncel ve endüstri standartlarına uygun bir arayüz yapılması tercih edilmiştir.

Bir sayaç üzerinden veri alınması için M-Bus protokolü kullanım senaryolarının anlamlandırılması, yazılım dilinde uygulama haline getirilmesi ve uzak sunucuya bu verilerin gönderilmesi, oluşabilecek sızma / manipülasyon yollarının anlaşılmasında büyük rol oynamıştır.

Aynı şekilde iOS mobil uygulaması geliştirilmesi sırasında SSL sertifikasının önemi veri güvenliğinde büyük katkı sağlamıştır. Aynı zamanda oturum (session) tabanlı bir kullanıcı doğrulamasının yapılması yerine JWT (JSON Web Token) doğrulaması yapılması işlemler sırasında oluşabilecek bug (hata) ve güvenlik tehtidi sayısını minimuma indirmesinde katkı sağlamıştır.

Veritabanı güvenliğinde ise sadece yerel makinenin erişim sağlayabileceği bir konfigürasyon yapılmış olup erişim güvenliği bu şekilde sağlanmıştır fakat herhangi bir güncelleme, bakım, müdahale durumu olduğunda çalışma sırasında bakım yapmak istediğinde uzaktan müdahale şansının olmadığı gözlemlenmiştir. Bu nedenle veritabanı güvenliği için ek bir uzak erişim talep sistemine ihtiyaç olduğu gözlemlenmiştir. Bu uygulama sayesinde yetki almak isteyen kişi için talep ettiği saatlerde ihtiyacı olan kullanıcı üretilebilir ve süre sonunda kullanıcı tekrar silinebilir, bu tarz erişim / yetki talepleri bankacılık sistemlerinde yoğun olarak kullanılmaktadır.

Open Web Application Security Project (OWASP) üzerinde raporlanan kaynak koda dayalı oluşabilecek tüm tehditlerin incelenmesi ve kod analizi yapabilen SonarQube ürünü ile uzak sunucu üzerinde çalışan Java uygulaması denetlenmiş olup sonuç ekranı Şekil 7.1'de gösterilmiştir.



Şekil 7.1. SonarQube Kod Analizi ve Kod Güvenliği Sonucu

KAYNAKÇA

[1] Y. Yang, L. Wu, G. Yin ve H. Zhao, «A Survey on Security and Privacy Issues in Internet-of-Things,» cilt 4, no. 5, 2017.

[2] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. . A. Savikko ve H. Leppäkoski, «Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey,» cilt 5, 2017.

[3] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal ve Q. Z. Sheng, «IoT Middleware: A Survey on Issues and Enabling Technologies,» cilt 4, no. 1, 2017.

[4] F. Ivan, T. Taleb, Y. Khettab ve J. Song, «A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems,» cilt 21, no. 1, 2019.

[5] G. Zhan, Y. Jiang, X. Yin ve S. Li, «Research on security of NB-IoT based on cryptography,» %1 içinde *2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE),* Changsha, China, 2021.

[6] M. F., «M-Bus Documentation Rev. 4.8,» [Çevrimiçi]. Available: https://www.m-bus.com.

[7] Pilot Elektronik, «PMM - 10 Ürün Özellikleri,» [Çevrimiçi]. Available: http://www.pilotelektronik.com/tr/urunler/pmm10.html.

[8] Quectel, «LPWA BG96 Cat M1/NB1/EGPRS,» [Çevrimiçi]. Available: https://www.quectel.com/product/lpwa-bg96-cat-m1-nb1-egprs/.

[9] Turkcell, «Turkcell NB-IoT Çözümleri,» [Çevrimiçi]. Available: https://www.turkcell.com.tr/kurumsal/kurumsal-cozumler/nb-iot.

[10] Alamofire Software Foundation, «Github - Alamofire,» [Çevrimiçi]. Available: https://github.com/Alamofire/Alamofire.

[11] B. Parno, A. Perrig ve V. Gligor, «Distributed detection of node replication attacks in sensor networks,» IEEE Symposium on Security and Privacy (S&P'05), 2005.