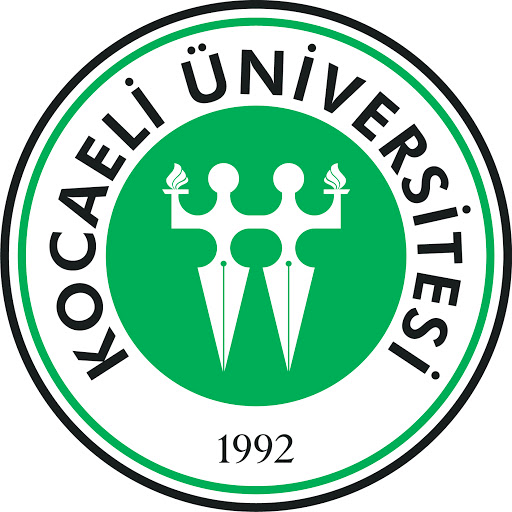
**KOCAELİ ÜNİVERSİTESİ**

**MÜHENDİSLİK FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**



**LİSANS TEZİ**

**ÇOKLU SUNUCULU NESNELERİN İNTERNETİ İÇİN DİJİTAL ADLİ BİLİŞİM VE MAKİNE ÖĞRENMESİ TEKNİKLERİ İLE SUÇ TESPİTİNİN YAPILMASI**

**YASİN EMİR KUTLU**

**5,2 cm**

**KOCAELİ 2020**

**KOCAELİ ÜNİVERSİTESİ**

**MÜHENDİSLİK FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

**BİTİRME ÇALIŞMASI**

**ÇOKLU SUNUCULU NESNELERİN İNTERNETİ İÇİN DİJİTAL ADLİ BİLİŞİM VE MAKİNE ÖĞRENMESİ TEKNİKLERİ İLE SUÇ TESPİTİNİN YAPILMASI**

**YASİN EMİR KUTLU**

**5,2 cm**

|  |  |
| --- | --- |
| **Doç.Dr.Kerem KÜÇÜK**  **Danışman, Kocaeli Üniv. -------------------------**  **Öğr. Gör. Uğur YILDIZ**  **Jüri Üyesi, Kocaeli Üniv. -------------------------**  **Arş. Gör. Dr. Meltem Kurt PEHLİVANOĞLU**  **Jüri Üyesi, Kocaeli Üniv. -------------------------** | |
|  |  |

**Tezin Savunulduğu Tarih: 24.06.2020**

**ÖZGEÇMİŞ**

Yasin Emir Kutlu 1997’de Malatya’da doğdu. Lise öğrenimini Tuzla Anadolu Lisesi’nde tamamladı. 2015 yılında girdiği Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü’nde halen eğitimini sürdürmektedir. Öğrenim hayatı içerisinde Erasmus+ Staj hareketliliği kapsamında Birleşik Krallık’ta çeşitli pozisyonlarda görev almıştır.

**ÖNSÖZ VE TEŞEKKÜR**

Bu tez çalışması, Nesnelerin İnterneti cihazları üzerinde Makine Öğrenmesi Tekniklerinin Evrişimsel Sinir Ağı Optimizasyonu ile Suç Tespiti ve bu teknoloji kapsamında geliştirilmiş cihazlar için Dijital Adli bilişim tekniklerinin kullanımı amacıyla gerçekleştirilmiştir.

Tez çalışmamda desteğini esirgemeyen, değerli fikirleriyle araştırma çalışmalarıma şekil veren, bana güvenen, yüreklendiren ve inancını ve desteğini hiçbir zaman yitirmeyen saygıdeğer danışmanım Doç.Dr.Kerem Küçük’e sonsuz teşekkürlerimi sunarım. Ayrıca projemizin gerçekleşmesinde bana vermiş olduğu fırsat ve şans için kendisine şükranlarımı sunarım.

Bu çalışmanın temellerinin atılmasına katkıda bulunan, değerli katkılarıyla çalışmalarıma yön veren, bana olan inancını, desteğini ve güvenini her zaman hissettiren saygıdeğer danışmanlarım Dr.Mo Adda’ya çalışmalarımı yürütmemde gerekli imkanları sağlayan Kocaeli Üniversitesine ve University of Portsmouth’a teşekkürlerimi sunarım.

Hayatım boyunca bana güç veren en büyük destekçilerim, her aşamada sıkıntılarımı ve mutluluklarımı paylaşan, her türlü imkanı benim öz gelişimim için seferber eden, eğitim hayatıma başladığım günden bugüne başarılı olacağıma inanan ve sonsuz destek veren sevgili aileme sonsuz teşekkürler ve minnetimi sunarım.

Haziran – 2020 Yasin Emir KUTLU

Bu dokümandaki tüm bilgiler, etik ve akademik kurallar çerçevesinde elde edilip sunulmuştur. Ayrıca yine bu kurallar çerçevesinde kendime ait olmayan ve kendimin üretmediği ve başka kaynaklardan elde edilen bilgiler ve materyaller (text, resim, şekil, tablo vb.) gerekli şekilde referans edilmiş ve dokümanda belirtilmiştir.

Öğrenci No: 150202040

Adı Soyadı: Yasin Emir KUTLU

İmza:

**İÇİNDEKİLER**

ÖNSÖZ VE TEŞEKKÜR i

İÇİNDEKİLER ii

ŞEKİLLER DİZİNİ iii

TABLOLAR DİZİNİ iii

KISALTMALAR DİZİNİ……………………………………………………………iii

ÖZET…………………………………………………………………………………iv

ABSTRACT v

GİRİŞ 1

1. METOD VE MATERYALLER 5

1.1. FORENSİK (ADLİ BİLİŞİM) UYGULAMALARININ TEMELLERİ 5

1.2 EVRİŞİMLİ SİNİR AĞLARI (CNN) ………………………………………11

1.3 RESİM VERİLERİ ÜZERİNDE OBJE SAPTAMA .……………………..12

1.4 IOT CİHAZ BİLGİSİ MODELİ …..……………………………………….13

1.5 IOT CİHAZLARINDAN ELDE EDİLMİŞ RESİM VERİ SETİ ………….13

2. ÇOKLU SUNUCULAR İÇİN IOT ADLİ BİLİŞİM 14

2.1. Cihazlar için Kayıt Oluşturma İşlemleri 16

2.2. IoT Cihaz Bilgilerinin Bulut Ortamında Saklanması 17

2.3. IoT Cihaz Takip ve Haritalama Algoritmaları 20

2.4 IoT Cihazlarındaki Resimlerin CNN Modeline Aktarımı…………………24

3. CNN TEKNİKLERİ KULLANILARAK IOT CİHAZLARINDAN SUÇ TESPİTİNİN GERÇEKLEŞTİRİLMESİ 24

3.1. Derin Öğrenme Metodolojileri ve Algoritmaları 24

3.2 Evrişimli Sinir Ağı Modeli ………………………………………………..26

3.4. IoT Cihazlarından Toplanmış Resimler Üzerinde CNN Modeli İle Sonuç Çıkarımı.. 28

3.4 Saptanmış Objelerin Sonuçlarının Bildirimi ………………………………28

4. İLGİLİ ÇALIŞMALAR 29

5. DENEYSEL ÇALIŞMALAR VE SONUÇLAR 29

6. KAYNAKLAR 30

EKLER 32

**ŞEKİLLER DİZİNİ**

Şekil G.0. Adli Bilişim Veri Gerekliliği Seviyelendirilmesi 3

Şekil 1.1.1. Adli Bilişim Metodolojilerinin Barındırdığı İşlem Basamakları 6

Şekil 1.1.2. Dijital Adli Bilişimin Katmanlı Yapısı 6

Şekil 1.2.1 Evrişimsel Sinir Ağı modelinin genel yapısı…………………………….12

Şekil 1.3.1 Silah, Bıçak ve Çiçek objelerinin saptanması ve sınıflandırılması ……..12

Şekil 1.4.1 IoT Cihaz DNA ve Gen Modeli …………………………………………14

Şekil 1.5.1 IoT Cihazlarından Elde Edilmiş Veri Seti ……………………………….14

Şekil 2.1.2 IoT cihazının masaüstü uygulaması ile bulut ortamına kayıt edilmesi…..17

Şekil 2.2.1. Günümüz Bulut Platform Kullanım Bilgileri 17

Şekil 2.2.2 Bulut Platform Mimarisi 18

Şekil 2.3.1 IoT Cihazlarının Lokasyon Değişikliklerinin Tutulduğu Özel Dosyalar .20

Şekil 2.3.2 IoT Cihazlarının Anlık Lokasyona Göre Harita Üzerinde Gösterilmesi 20

Şekil 2.3.3 Cihazların Lokasyon Değişikliği Sırasında Dosyaların İçerik Durumu 21

Şekil 2.4.1 IoT Cihazlarından Elde Edilmiş Resim Öğeleri…………………………22

Şekil 2.4.2 Ön işleme (Preprocessing) mekanizmasının yazılımsal ifadesi…………23

Şekil 3.1.1 ML çatısı altındaki öğrenim tekniklerini gösterimidir………………….24

Şekil 3.2.1 CNN Modelinin Katman Yapısı ……………………………………….26

Şekil 3.2.2 CNN Modelinin Epoch Sayısına Göre Doğruluk Yüzdesi Grafiği …….27

Şekil 7.1 IoT Cihaz Kayıt İşlemi ………………………………………………….31

Şekil 7.2 Başarısız Cihaz Kayıt İşlemi Hata Mesajı ……………………………...32

Şekil 7.3 Login Penceresi ………………………………………………………...32

Şekil 7.4 IoT Cihaz Soruşturma Penceresi …………………………..…………...33

Şekil 7.5 IoT Cihaz Soruşturma Sonuç Bildirimi …………………………..….....33

**TABLOLAR DİZİNİ**

Tablo 1.0. Adli Bilişim Alt Dalları 5

Tablo 1.1.3. IoT Adli Bilişim ile Geleneksel Adli Bilişim Karşılaştırılması 8

Tablo 2.1 Ana ve Alt Sunucuların Kodları…………………………………………...15

Tablo 2.1.1.DNA Modeli 16

Tablo 3.1. Makine Öğrenmesi, Yapay Zeka ve Derin Öğrenme Arasındaki İlişki 23

**Kısaltmalar**

IoT : Nesnelerin İnterneti

DI : Dijital Soruşturma (Dijital Investigation)

ML : Makine Öğrenmesi (Machine Learning)

AI : Yapay Zeka (Artifical Intelligence)

DL : Derin Öğrenme (Deep Learning)

IEEE : TheInstitute of ElectricalandElectronicsEngineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)

CNN : Evrişimsel Sinir Ağları (Convolutional Neural Network)

**ÇOKLU SUNUCULU NESNELERİN İNTERNETİ İÇİN DİJİTAL FORENSİK VE NESNELERİN İNTERNETİ CİHAZLARI İÇİN SUÇ TESPİTİ**

**ÖZET**

Bu çalışmanın amacı, geride bıraktığımız on yıllardan beri kullanımı oldukça yaygınlaşan Nesnelerin İnterneti cihazlarını çoklu sunucular üzerinde çalıştırmak, çalışan cihazlar üzerinden toplanan verilerden suç tespiti yapabilmek için gerekli tekniklerin ve algoritmaların kullanılmasını sağlamaktır.

İlk olarak, sistem üzerinde çalışan her ülkenin birer adet ana sunucusu bulunmaktadır. Şehirler ise bulundukları ülkelerin hiyerarşik olarak alt sunucularını oluşturmaktadır. Böylelikle alt sunucular ve ana sunucu bir bütünü temsil etmektedir. Piyasadan satın alınmış bir Nesnelerin İnterneti cihazı, bulunduğu şehirin sunucusuna kayıt edilmek zorundadır. Kayıt aşamasında cihazın ve cihazı kullanan kişilerin gerekli bilgileri sisteme yetkililer tarafından kayıt edilmelidir. Bu işlemin ardından, cihaz kullanıma hazırdır. Sisteme kayıtlı olan tüm cihazların delil olma potansiyelindeki verileri (resim, email, kredi kartı bilgisi, arama geçmişi vb.) farklı bir bulut ortamında sadece okunabilme özelliği ile saklanmaktadır.

Bu çalışma gereğince, bulut platforma kayıt edilmiş ve kullanıcılar tarafından faal olarak kullanılan her bir cihazın sağladığı verilerin suç tespiti için incelenmesinin gerektiği aşikardır. Bununla alakalı olarak, bir üst parağrafta belirtilen delil olma potansiyeli olan veriler arasında bulunan kullanıcı tarafından çekilen resimler üzerinde makine öğrenmesi teknikleri kullanılarak suç tespiti gerçekleştirilmeye çalıştırılacaktır. Bulut üzerinde kayıtlı halde bulunan cihazların zaman içerisinde sağlayacakları bileşenler her bir cihaz ile eşleşmiş delil depolama alanlarında tutulmaktadır. Bireylerin sağlamış olduğu bu veriler, kişisel veri gizliliği ve hassas bilgiler içerdiğinden gerekli bir husus olmadığı takdirde hiçbir kurumla paylaşılmayacaktır.

Geliştirilmesi planlanan bu yeni sistem ile, günümüzde kullanımı oldukça yaygınlaşan akıllı cihazların daha güvenilir bir ortamda kullanılması, bu cihazları kullanan insanların oluşabilecek tehditlerden uzak tutulması ve suçluların en kısa sürede tespitin yapılıp gerekli adli kuruluşlara teslim edilmesi amaçlanmaktadır. Bu çalışmaya bağlı olarak, IoT teknolojileri ile birlikte Bulut Bilişim teknolojileri ve Makine Öğrenmesi tekniklerinin uygulanması planlanmaktadır.

**Anahtar kelimeler:** Nesnelerin İnterneti, Dijital Forensik, Makine Öğrenmesi, Forensik Analizi, Dijital Soruşturma.

**DIGITAL FORENSICS FOR IoT MULTIPLE SERVERS AND CRIME DETECTION FOR IoT DEVICES**

**ABSTRACT**

The aim of this study is to run the Internet of Things devices on multiple servers over the last 10 years and to use the necessary techniques and algorithms to detect crime from the data collected from the working devices.

First, each country running on the system has one main server. Cities constitute the sub-servers of the countries in where they are located. Thus, the sub-servers and the main server represent a whole component. An Internet of Things device purchased on the market field must be registered on the server of the city where it is located. During registration, the necessary information of the device and the persons using the device should be recorded by the authorities in the system. The appliance is now ready for use. The data (picture, email, credit card information, call history, etc.) of all devices registered in the system with the potential to be evidence is stored in a different cloud environment with readability only.

As a result of this study, it is evident that the data provided by each device registered to the cloud platform and used actively by users should be examined for crime detection. Related to this, crime detection will be attempted by using machine learning techniques on the pictures taken by the user among the data which have the potential to be evidence mentioned in the upper paragraph. The components that the devices registered in the cloud will provide over time are kept in the evidence storage areas paired with each device. Since the data provided by individuals contains personal data confidentiality and sensitive information, it will not be shared with any institution unless necessary.

With this new system, which is planned to be developed, it is aimed to use smart devices which are widely used in a more reliable environment, to keep the people using these devices away from possible threats and to ensure that the criminals are detected and delivered to the required judicial institutions as soon as possible. Based on this study, it is planned to implement Cloud Computing technologies and Machine Learning techniques along with IoT technologies.

**Keywords:** Internet of Things, Forensics, Machine Learning, Forensics Analysis, Digital Investigation.

**GİRİŞ**

Nesnelerin interneti günümüz internetinin farklı bir modelidir. Geride bıraktığımız son on yılda yapılan yüksek bütçeli yatırımlar sayesinde gelişimine oldukça yüksek hızla devam eden bu yeni teknoloji insan hayatının oldukça büyük bir kısmına yayılmış durumdadır. Bunlara ek olarak, günümüz bilgisayar bilimlerindeki gelişmeler ve değişimlerde bu sektörün gelişiminde önemli bir paya sahiptir. 1991 yılında University of Cambridge’de görev yapmakta olan yaklaşık 15 akademisyenin kendi aralarında geliştirdikleri kameralı kahve makinesi izleme sistemi bu teknolojideki ilk adım olarak değerlendirilmiştir. 2000’li yılların başları sayılabilecek bir zamanda tanıtılan RFID teknolojileri ile gelişen bu eğilime yön verici nitelikte olmuştur.

Bilişim teknolojilerinin günden güne son hızla gelişmesi yeni teknolojilerinde gelişmesinde önemli bir paya sahiptir. Günümüzde ise IoT teknolojileri farklı formlarda önümüze çıkmaktadır. Örnek olarak, Akıllı şehirler, evler, cihazlar, hasta takip sistemleri, verimli enerji sistemleri, sensörler, bulut bilişim platformları, gömülü sistemler ve birçok farklı alanda etkisi görülmektedir [1]. Gelecek yüzyıldaki bilişim teknolojileri ve telekomünikasyon hizmetlerinin dünya genelinde daha da yaygınlaşması ve farklı alanlar üzerindeki gelişimi araştırmacılar tarafından beklenmekte ve her geçen gün çalışmalar hızlı bir biçimde sürmektedir. Bununla beraber yazılım araç ve gereçlerinin nesnelerin internetinin gelişimine büyük bir katkı sağlayacağı aşikardır. Bu bilgiler ışığında, kullanımı her geçen gün artan IoT cihazları için ortaya çıkabilecek problemlerden bir tanesi de güvenlik problemidir. IoT cihazlarının ilerleyen yıllardaki beklenen gelişimi göz önüne alındığı takdirde, günümüz ortamında bazı tekniklerin geliştirilerek bahsi geçen bu cihazların oluşturabileceği potansiyel tehditler kontrol altına alınmalıdır.

Nesnelerin interneti (IoT) üzerindeki gelişmeler aynı zaman dijital forensik alanındaki açıkları ve üzerinde çalışılması gerek konu sayısını da artırmaktadır. Bilim insanları tarafından yapılan sayısız araştırmalar bizlere dijital forensik tekniklerinin nesnelerin interneti uygulamaları üzerinde ve forensik soruşturmalarının bu alan ışığında nasıl uygulanacağı konusunda yol gösterici olmaktadır [2].

Her geçen gün yaygınlaşan bilişim suçları, araştırmacıları, adli bilişim uzmanlarını ve hükümetlerin üzerinde çalışılması gereken bir önemli bir konu başlığı haline gelmiştir. Bu kapsamda özellikle Avrupanın önde gelen ülkelerinde ve Amerika Birleşik Devletlerinde ciddi araştırmalar ve yatırımlar yapılmaktadır. Son yıllarda gelişen IoT teknolojileri ve bununla aynı paralalde gelişme gösteren siber güvenlik çalışmalarıyla beraber kötü niyetli yazılımlar, virüsler ve sanal tehditler gibi kavramların adları sıklıkla akademik çalışmalar içerisinde geçmeye başlamıştır. Bu kapsamda, üretilen kötü amaçlı yazılımların IoT teknolojilerinin kullanmış olduğu ağ alt yapısını nasıl etkileyeceği ve siber güvenlik üzerindeki endüstriyel ve akademik çalışmalar son hızla sürmektedir. Bilim insanlarının günümüzde halen üzerinde çalışma yaptığı konular olmasına karşın kişisel veri güvenliği ve gizlilikte dikkat edilmesi diğer bir araştırma konusudur. Buna bağlı olarak, bu çalışmada öne sürülen modelde ve içerisinde barındırdığı yazılımsal ve mantıksal yapılar da kişisel veri güvenliği ve gizliliği en yüksek önceliği sahiptir.

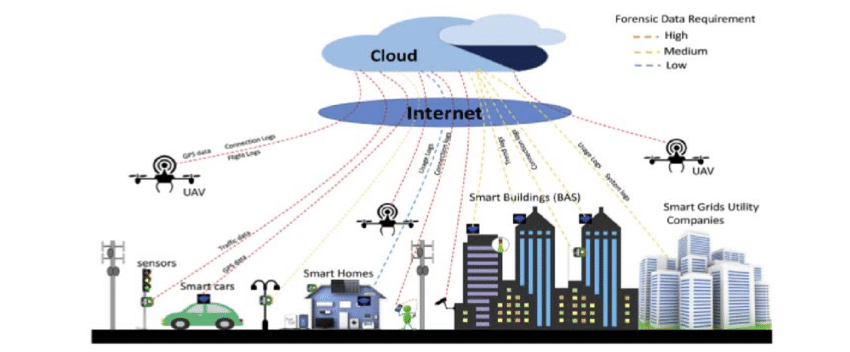
Bu çalışma gereğince, belirlenmiş olan 6 ülke (Türkiye, Birleşik Krallık, Fransa, Almanya, İtalya, İspanya) kapsamında sanallaştırılmış ana sunucular ve bu ülkelerin hiyerarşik olarak alt katmanında bulunan 12 farklı şehirde kurulmuş alt sunucular öne sürülen modelin genel yapının iskeletini oluşturmaktadır. Her bir şehir bulunduğu ülkenin ana sunucusuna bağlıdır. Şehirlerde bulunan alt sunucular altında her biri *Evrensel Kimlik Numarasıyla (UIDN)* kayıtlı IoT cihazlarını saklamaktadır.

Geride bıraktığımız son on yıl içerisinde hayatımızda birçok farklı alanda artan akıllı cihaz kullanımı, bu cihazların bilgilerinin tutulduğu veritabanı sistemlerinin özenle hazırlanması gerekliliğini kaçınılmaz kılmıştır. Bu kapsamda gerekliliklerin etkili bir yolla gerçekleştirilmesi için planlanan veritabanı modelinde ayrıklaştırılmıştır bir mimari kullanılmıştır. Böylelikle yüksek derecede anlaşılırlık ve verimli bir yazılım altyapısı hedeflenmiştir. Sistem üzerinde kayıtlı cihazların kimlik numaraları belirlenirken her bir cihaza eşsiz bir tanınma numarası atanmıştır. Bu numaranın belirlenmesi sırasında *Ülke Kodu, Şehir Kodu, Cihaz Sıra Numarası* parametreleri kullanılmıştır. Böylelikle her bir cihaz için eşsiz olan bir kimlik numarası belirlenmiştir.

Cihazların bulut ortamına kayıt işlemi yapılırken belirli bilgilerin kullanıcılardan alınması gerekmektedir. Bu işlem sırasında, kullanıcıların kişisel bilgileri *DNA* modeline benzetilmiştir. Herhangi bir akıllı cihazın sisteme kayıdı sırasında *Cihaz Sahibinin Adı, Cihaz Kullanıcısının Adı, Cihazın Seri Numarası, Cihazın IMEI numarası, Anlık IP Adresi, Cihazın bulunduğu noktanın Enlem ve Boylam Bilgisi’*nin sisteme girişi zorunludur. Böylelikle cihazın kullanımı sırasında suç teşkil edecek herhangi bir durumla karşılaşıldığında, cihazın ve kullanıcısının takibinin sağlanması kontrol altına alınacaktır.

Cihazların kayıt altında tutulduğu veritabanının bulunması, yazılımsal ve mantıksal sistemlerin kurulması ve gerekli algoritmaların çalıştırılması için yeterli değildir. Buna ek olarak, cihazların kimlik numaralarıyla eşleşmiş veri depolarında delil olma niteliğine sahip verilerin tutulması gerekmektedir. Cihazların tutulduğu veritabanında cihazların kendilerine has verilerin aynı bloklarda saklanması büyük orandaki verilerin bir arada tutulmasına ve bununla beraber çok karmaşık bir veritabanı dizaynına yol açacağından bu veriler farklı veritabanları içerisinde saklanmaktadır. Buna ek olarak, IoT cihazlarının kullanıcı kaynaklı fiziksel hasar sonucu oluşabilecek önemli verilerin kaybını önlemek ve cihazlar yok edilse dahi, delillerin kaybolmaması için soruşturmalar açısından kritik bir değere sahip bilgilerin bulut ortamında saklanması gerekmektedir. Bu yöntem ile IoT cihazlarından elde edilmiş büyük verilerin korunması başarıyla sağlanabilecektir. Delillerin tutulduğu veri tabanının diğer veritabanlarından ayıran belirli özellikleri vardır. Bunların en başında, bu veritabanında sadece okuma (read) işleminin yapılabiliyor olmasıdır. Bunun işlemin nedeni, delil bilgilerinin saklandığı veritabanı sistemine dışarıdan bir erişim ile bağlanıldığında herhangi bir kullanıcının kişisel veri bloğu işgal edilip kötü niyetli insanlar tarafından istismar edilmesini engellemek ve saklanan verinin doğruluk değerini korumaktır. Cihazların sağladığı verilerin adreslenmesinde *Evidence* veritabanının *Web API* anahtarı cihaz bilgileri ile birlikte saklanmaktadır. Böylelikle yüksek performanslı, güvenli ve algoritmaların çalıştırılabileceği yazılımsal bir ortam elde edilmektedir.

Akıllı cihazlar ve son hızla gelişmekte olan IoT teknolojileri büyük veri (Big Data) alanında da gelişme göstermeye son derece açıktır. Dünya üzerinde 2020 yılında kullanılacak IoT cihazı sayısı 8.4 milyara ulaşması beklenmektedir. Bu sayının 2022 yılı itibariyle 20.4 milyara ulaşması beklenmektedir [3]. Bu veriler, yapılmış olan bu çalışmanın doğrudan büyük verilerle ilişkisel olacağını gözler önüne sermektedir. Bu anlayıştan yola çıkarak, mimari yapı üzerinde kayıtlı olan her bir cihazın incelenmesi (Examination) hususunda gerekli olan yetkili soruşturmacıların (Investigator) sisteme kayıtlı olması gerekliliğini göstermektedir.



Şekil G.0 Akıllı Şehirlerde Ağırlık Değerlerine Göre Adli Bilişim Kaynakları [4]

Bu kapsam doğrultusunda, veritabanı üzerinde devlet makamları tarafınca yetkilendirilmiş dijital forensik polislerinin gerekli bilgiler ile birlikte hesaplarının veritabanında depolanması gerekmektedir. Soruşturma polislerinin bilgilerinin yazılım mimarisi üzerinde tutulması sırasında ülkeler polislerin *isim, soyisim, mertebe,* ve *güvenirlik seviyelerini* geliştirilmiş olan yazılım arayüzüne sağlamakla yükümlüdür. Güvenirlik seviyesi, polislerin yapacağı soruşturmaların sonucuna olan itibarı ve ülkeler arası veri transferini etkileyebilir. Soruşturma polislerinin veritabanı üzerinde kayıtları oluşturulurken *ülke kodu, şehir kodu, mertebe kodu* ve *sıra numarasına* göre oluşturulmuş birer adet eşsiz kimlik numarası bulunmaktadır. Müfettişler bu kimlik numaraları ile birlikte geliştirilmiş olan yazılım arayüzüne giriş yapıp mahkeme kararıyla elde etmiş oldukları izinleriyle IoT cihazlarından elde edilmiş delilleri 24 saat içerisinde inceleyebilirler. Cihazların incelenmesi sırasında mahkeme emriyle gönderilmiş bir kod yardımıyla, polisler cihazlar üzerinde çalışabilir ve IoT cihazlarından elde edilmiş görsel verileri inceleyebilirler. Sürenin dolmasıyla beraber kişisel verilerin gizliliği nedeniyle sistemden uzaklaştırılırlar. Soruşturma polisleri daha fazla zamana ihtiyaç duyduklarında ise yeni bir mahkeme kararının çıkmasını beklemek ile yükümlüdürler.

**1. METODLAR VE MATERYALLER**

**1.1 FORENSİK (ADLİ BİLİŞİM) UYGULAMALARININ TEMELLERİ**

Teknolojinin özellikle geride bıraktığımız son 20 yıl boyunca hızla gelişmesine bağlı olarak bilgisayarlar, cep telefonları ve diğer cihazların kullanımı oldukça yaygınlaşmıştır. Günümüzde toplumlarının hemen hemen her kesiminde teknolojinin kullanımı her yaş aralığında yoğun bir şekilde devam etmektedir. Bu bağlamda, suç işleme niyetinde olan kişi veya kurumlarında aktifliği her geçen artmaktadır. Teknolojiyi kullanan insanların fiziksel ve manevi güvenliğini sağlamak, üzerinde çalışma yürütmek, elektronik cihazları ve bu cihazlardan sağlanmış verilerin incelenmesi alanında kullanılan ve yol gösterici kabul edilen bilim dalına Dijital Adli Bilişim (Digital Forensics) adı verilir. Her geçen gün teknolojinin gelişmesi ve farklı dallara ayrılması dijital adli bilişiminde kendi içerisinde dallanmasına neden olmuştur. Bununda yanında, geçmişte ve günümüzde popüleritesini koruyan ve dijital adli bilişim ile koordineli çalışan bir bilim dalıda Geleneksel Adli Bilişimdir. Bu bilim dalı dijital adli bilişimin aksine kriptoloji, seroloji, zehir bilimi (Toxicology) ve doküman soruşturmaları gibi konular üzerinde çalışır.

|  |  |
| --- | --- |
| Bilgisayar Adli Bilimi | Computer Forensics |
| Dosya Sistemi Adli Bilimi | **File System Forensics** |
| İşletim Sistemi Adli Bilimi | **OS Forensics (Windows, Linux, IOS)** |
| Ağ Adli Bilimi | **Network Forensics** |
| Mobil Cihaz Adli Bilimi | **Mobile Forensics (Android, IOS)** |
| Kötü Yazılım Adli Bilimi | **Malware Forensics** |
| Geçici Bellek Adli Bilimi | **Memory Forensics** |

Tablo 1.0 Adli Bilişim Alt Dalları [5]

* 1. **Dijital Adli Bilişim Metodolojisi ve Soruşturma Modeli**

Dijital adli bilişim metodolojisi kendi içerisinde bulundurduğu prosedür ve işlemler için bir mimari yapı barındırmaktadır. Günümüz adli bilişim teknikleri için standartlaşmış bir yöntemden bahsetmek mümkün değildir. Fakat buna karşın, her bir yaklaşım temelde aynı basamakları içermektedir. Bu basamaklar *soruşturma başlatmak, soruşturma hazırlıklarını tamamlamak, Değerlendirme yapmak, IoT cihazlarından veri toplamka, analiz etmek, çıkarım geliştirmek, sonuçları sunnma* şeklinde standartlaştırılabilir. Bu tekniklerin kullanımı soruşturmacılar tarafından adli bilişim metodolojisine bağlı kalınacak şekilde farklı şekilde kullanılabilir. Bazı metodlar soruşturmaya başlamadan önce planlanmış bir hazırlık işlemi geçirmeyi mecburi kılarken bazı teknikler kendi içerisinde almış olduğu şekil gereği öncel bir hazırlık istemeden kendi içerisindeki farklı teknik basamaklar içermektedir. Bunlara örnek olarak, Bilgisayar Adli Bilişimi alanında uygulanan *Kimlik Saptama (Identification)* işlemi örnek gösterilebilir. İşlemlerin boyutu, uygulanış şekli ve soruşturmacının stili ne olursa olsun, izlenen süreçler adli bilişim tekniklerine uygun yapılmaktadır.

Şekil 1.1.1 IoT Cihazları İçin Dijital Adli Bilişim Soruşturma ve Analiz Döngüsü .[6]

Başlangıç : IoT cihazının soruşturulmasının nedeni ve amaçlarının yetkili organlara bildirildiği kısımdır.

Hazırlık : Ekipman ve adli bilişim uzmanlarının toplanması, buna ek olarak yetkili birimlerin soruşturmaya onay vermesi işlemidir.

Değerlendirme : Veri ve kişisel kaynakların, cep telefonu, bilgisayar, tablet ve bulut bilişim ortamının bunlara ek olarak ise potansiyel delil olma niteliğindeki kaynakların belirlenmesi.

Veri Toplama : Veri tanımlandıktan sonra adli bilişim teknikleri ile ele alınmalıdır. Örneğin, cep telefonundan elde edilmiş bir resmin yetkili otoritelerce saklanarak incelenmesi bu işleme örnektir. Bunun yanında, elde edilmiş toplam verilerden gerekli olmayanların bu kümeden çıkarılarak en net veri kümesi halinin elde edilmesi gereklidir. Bu işlerin tamamı bu safhada gerçekleştirilerek incelenecek net veri kümesi oluşturulur.

Analiz : Veri alt kümeleri ve IoT cihazlarından elde edilmiş potansiyel kanıtların odak noktası olarak belirlenip devamında incelendiği aşamadır. Soruşturma devam ederken eğer yeni bir cihaz bulunursa o cihaz için aynı işlemler birinci aşamadan başlanarak tekrarlanır.

Çıkarım Geliştirme : Analiz sürecinin tamamlanmasının ardından elde edilen bilgiler için kim, nasıl, ne zaman, neden ve nerede sorularına cevap arandığı ve fikirlerin oluşturulduğu kısımdır. Bu aşamada elde edilen fikirler IoT cihaz soruşturmasının ilerleyen adımlarında kanıt ve istihbarat ile ilgili soruları cevaplamak için kullanılır.

Sunum : Analiz sürecinin genel sonuçları bir rapor halinde yetkili birimlere sunulur. Bu aşamanın sonunda IoT cihaz soruşturmasının doğru şekilde sonuçlandığından emin olmak gerekir. Özetle, yapılan IoT cihaz soruşturmasının genel hatlarıyla değerlendirilip yetkili makamlara sonuçların iletildiği bölümdür. Bu süreç içerisinde gerekli farklı görevler tanımlanırsa yapılacak olan tüm işlerin tamamlanması sonucunda gerekli rapor hazırlanır ve yetkili makamlara IoT cihazının soruşturma raporu teslim edilir.

Herhangi bir adli bilişim soruşturmasında görev alan dijital adli bilişim görevlileri suç mahalli ile ilgili delilleri korumalı, gerektiğinde fotoğrafını çekmeli ve yetkili mahkemelerin delillerden karar çıkarabilmesi için gerekenleri yapmakla yükümlüdür. Bir soruşturmanın en önemli kısmı delillerin toplanması ve toplanmış verilerin korunmasıdır. Soruşturmaların bütünlüğü gereği IoT cihazlarından toplanmış ve potansiyel delil niteliğinde olan her bir veri bilişim uzmanları tarafından dijital adli bilişim teknikleri yardımıyla incelenip bir sonuç çıkarılmalı ve gerekli görülen durumlarda yetkili soruşturma amirlerine bilgi verilmelidir. Bu döngü içerisinde bilişim görevlilerinin amacı elde edilen verilerin derinlemesine incelenmesidir. Tarihsel olarak, siber suçlar ve bilişim suçları geri bıraktığımız yıllarda fazla popüler olmasada özellikle yeni gelişen teknolojiler ve yapılan yatırımlar sayesinde her geçen gün oransal olarak artmaktadır. İşlenen suçların tespiti sırasında adli bilişim soruşturmasının katmanlı yapısı senaryoların aydınlatılmasında ve görselleştirilmesinde önemli bir yere sahiptir. Şekil 1.1.2 de dijital adli bilişimin katmanlara ayrılmış yapısı şematize edilmiştir.

|  |  |  |
| --- | --- | --- |
| call, cell, communication, interface, multimedia, phone, telephone iconlaptop, notebook, pc icon    Katman 1  İç Ağ Yapısı | Katman 2  Ağ Geçidi (Gateway) | cloud icon  Katman 3  Dış Ağ Yapısı (Cloud) |

Şekil 1.1.2 Dijital Adli Bilişimin Katmanlı Yapısı [7]

Şekil 1.1.2 de gösterilmiş katmanlı yapı baz alınarak yapılan yaklaşımlar yapılan çalışmanın temellerini oluşturmaktadır. Bu yapıda gösterilmiş katman 1 IoT cihazlarından (Telefon, Bilgisayar, tablet vb.) oluşmuş yapıyı temsil etmektedir. Katman 2 ise IoT cihazları ile verilerin depolandığı katman 3 arasındaki köprü bağlantısını temsil etmektedir. Son olarak, şemanın en son katmanını temsil eden katman 3 ise sanallaştırılmış ana sunucuları ve alt sunucuları temsil etmektedir. Bu katman sisteme kayıtlı tüm bileşen bilgilerini sakladığı için içerisinde çok büyük bir veri topluluğu içerir. Bu katmanın içerisinde her bir alt sunucuya kayıtlı cihazın ülke, şehir, cihaz bilgisi, kullanıcı, sahip ve diğer bilgiler saklanmaktadır. Bunlara ek olarak, sistemin bir paydaşı olan soruşturmacıların bilgileride bu servislerde tutulmaktadır. Ayrıca, IoT cihazlarından sağlanmakta olan ve delil potansiyeli taşıyan veriler (resim, email, kredi kartı bilgisi, rehber bilgileri vb.) bu katman içerisinde özel olarak dizayn edilmiş veri satırlarında saklanmaktadır. Şemadan rahatlıkla anlaşılabileceği gibi her katman sistemin önemli bir parçasıdır ancak katman 3 üzerinden sağlanacak veriler dijital adli bilişim için çok daha fazla büyük önem arz etmektedir. Buna karşın, geleneksel adli bilişim metodları katmanlı yapıdan farklı bir mimari yapı üzerinde kurulmuştur. Son 20 yılda önemli gelişmeler kat eden dijital adli bilişim, geleneksel modele göre günümüz teknolojileri ile daha uyumlu çalışmaktadır. Teknik bakımdanda geleneksel ve dijital modelin ayrıştığı konular bulunmaktadır. Bu 2 farklı modelin detaylı karşılaştırılması şekil 1.1.3’de şematize edilmiştir.

Bu tablodan anlaşılabileceği üzer IoT adli bilişim günümüz teknolojileri ile daha uyumlu çalışmaktadır. Bu savı tezlemek amacıyla IoT adli bilişim teknik ve teknolojilerinin günümüz gelişen veri bilimi ve büyük veri konusunda daha esnek çalışabildiği rahatlıkla söylenebilir. Ayrıca, IoT adli bilişimi günümüzde popüleritesini koruyan RFID teknolojilerinin soruşturulması konusunda da aktif olarak başvurulan metodları içermektedir. Bu bilim dalının en önemli paydaşlarından olan delil (evidence) bileşenleri IoT forensik alanında daha geniş bir yayılım göstermektedir.

Buna karşın geleneksel yöntem, dijital adli bilişime göre daha sığ bir çalışma alanına sahiptir. Bunun getirmiş olduğu dezavantaj ile dijital adli bilişim her geçen gün hızla gelişmekte, incenlenmesi gereken veri sayısı hızlıca artmaktadır. Bu iki yöntem benzerlik konusunda kıyaslandığında ise hukuksal ve kimler tarafından yapılabileceği hakkında aynı paydaşlar üzerinde sonuçlar vermektedir. Öte yandan günümüz yazılım yapıları ve kodlanabilir yapıların hızlıca gelişmesi dijital adli bilişimin önünü oldukça açmaktadır. Bu çalışmada yapıldığı üzere, Evrişimsel Sinir Ağı modeli ile birleştirilen IoT modeli sonucunda dijital adli bilişim uzmanları için daha hızlı ve doğru karar verme mekanizması oluşturulmuştur. Bu ve benzer fikirler ile bakıldığında her geçen gün oldukça hızlı bir biçimde gelişen yazılım, bilgisayar bilimleri ve teknoloji dünyası dijital adli bilişimin gelişmesinde önemli bir paya sahiptir.

|  |  |
| --- | --- |
| **IoT (Dijital) ve Geleneksel Adli Bilişim Karşılaştırması** | |
| **Geleneksel Model** | **Dijital Model** |

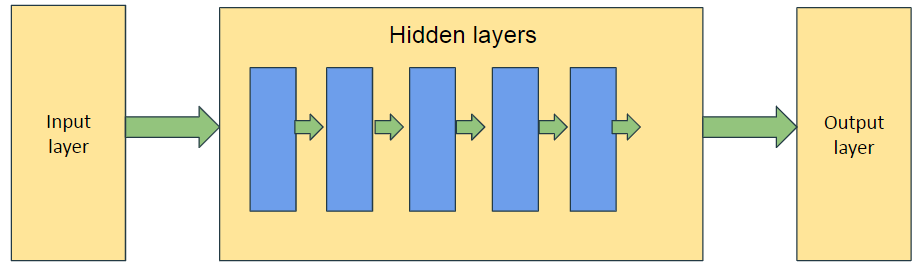
|  |  |  |
| --- | --- | --- |
| **Delil Kaynakları** | Bilgisayarlar, Mobil cihazlar, fiziksel dökümanlar, ağ geçitleri vb. | Akıllı ev uygulamaları, mobil cihazlar, arabalar, etiketler, sensörler, tüm IoT teknolojilerinden elde edilmiş fiziksel ürünler. |
| **Yargı Yetkisi** | Bireyler, şirketler ve hükümetler. | Geleneksel model ile aynı. |
| **Cihaz Sayısı** | 1 Milyon civarında cihaz. | 2020 yılı itibariyle 50 milyon civarında cihaz. |
| **Delil Tipi** | Elektronik dökümanlar, standart dosya formatları. | Elektronik dokümanlar ve herhangi bir formattaki dosyaların tümü. |
| **Kullanılan Ağ Tipi** | Kablolu, kablosuz, bluetooth, internet ve mobil haberleşme kanalları. | RFID, sensör ağları. |
| **Veri ve Delillerin Miktarı** | Terabayt boyutunde veri. | Eksabayt boyutunda veri. |
| **Sahiplik** | Bireyler, gruplar, şirketler, hükümetler. | Geleneksel model ile aynı. |
| **Ağ Sınırları** | Açık olarak sınırlandırılmış bir ağ yapısı. | Sınırları her geçen gün büyüyen bulanık bir ağ yapısı. |

Tablo 1.1.3:IoT Adli Bilişim ile Geleneksel Adli Bilişim Karşılaştırılması. [8]

Bu tablodan yola çıkarak belirli yorumlar yapılabilir. Bu bağlamda IoT (dijital) adli bilişimin her geçen gün daha da büyüyerek teknolojij hayata girdiğini söylemek mümkündür. Fakat bununla beraber yeni gelişiminin getirmiş olduğu bazı dezavantajlarında olduğunu söylemek mümkündür.

Sonuç olarak, bahsedilen bu yaklaşımların tamamının bulunduğu yazılımsal bir mimari gerekli kabuller yapılarak inşa edilmiştir. Yazılım mimarisinin gelecek geliştirmeleri karşılaşması ve yüksek performanslı soruşturma imkanı sunabilmesi için gerekli önlemler ve yapılar inşa edilmiştir. Bu kapsamda öngörülen iyileştirmeler ve tasarlanmış model 2. bölümde Çoklu Sunucular için IoT adli bilişim başlığı altında incelenmiştir.

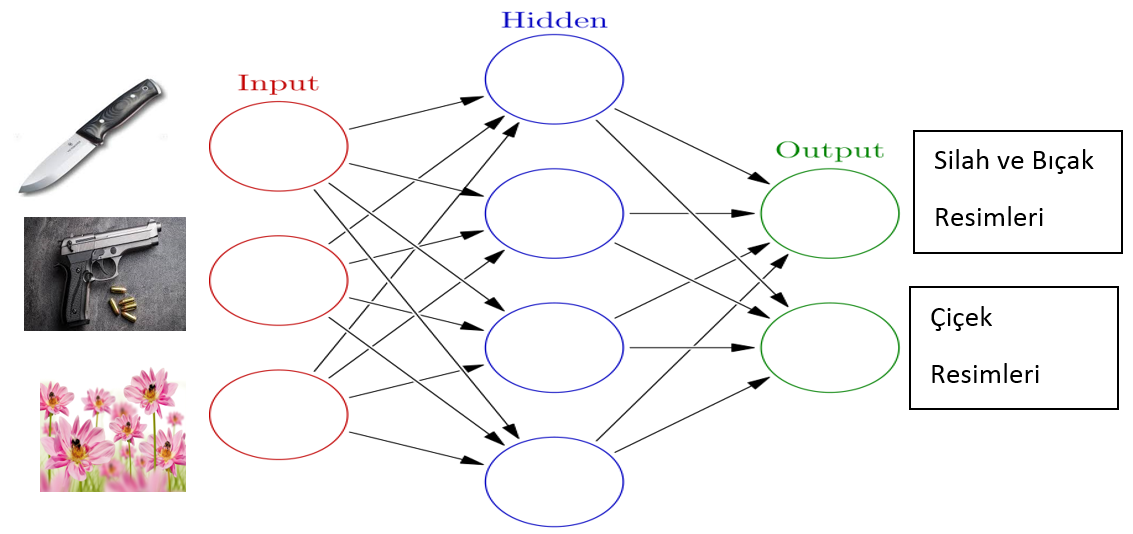
**1.2 Evrişimsel Sinir Ağları (CNN)**

Evrişimsel sinir ağları girdi (input) olarak bir görüntü alıp, almış olduğu bu görüntüdeki nesneleri veya çeşitli görüntüleri birbirinden ayırabilen ve sınıflara bölebilen bir derin öğrenme algoritmasıdır. Bu modeller genel olarak görüntü sınıflandırma, obje tanıma ve görüntüler arası benzerlik bulma işlemlerini yapan sinir ağlarıdır. Bu ağların çalışma yapısı basitçe üç temel sınıfa dayanır. Bu sınıflar, input layer, output layer ve hidden layers dır. Katmanlardan oluşan sinir ağları input olarak aldığı bir veriyi içerisinde barındırdığı çeşitli katmanlardan geçirerek output layer vasıtasıyla çıkışında bulunan sınıflara gönderir. Bu katmanlar içerisinde matematiksel işlemlerin yapıldığı birer aktivasyon fonksiyonu olarak düşünülebilir. Model içerisindeki her bir katmanın çıktısı bir sonraki katmanın girdisi konumundadır. Şekil 1.2.1’de CNN modelinin genel yapısı gösterilmiştir.

Şekil 1.2.1 : Evrişimsel Sinir Ağı modelinin genel yapısı

Şekil 1.2.1 ‘ de gösterilmiş olan CNN modeli için bazı kavramların açıklanması gerekmektedir. Input (Giriş) katmanı, resim verilerinin girdi olarak kabul edildiği ve modelin ilk katmanı olarak değerlendirilir. Input katmanın da işlenmiş olan veriler bir sonraki katman olan Hidden (Gizli) katmana yönlendirilir. Bu aşama içerisinde bir takım sinir hücresinden geçen resim verileri işlenerek Output (Çıktı) katmanına yönlendirilir. Output katmanı ise, resim verilerinin işleneceği son yapıdır. Bu katmanın görevi resimleri uygun sınıflara bölmektir. Yazılımsal olarak bu işlev Dense fonksiyonu ile belirlenen küme sayısına göre işlenmiş resimler belirlenen sınıf sayısınca karar verilerek sınıflandırma işlemi tamamlanmış olur.

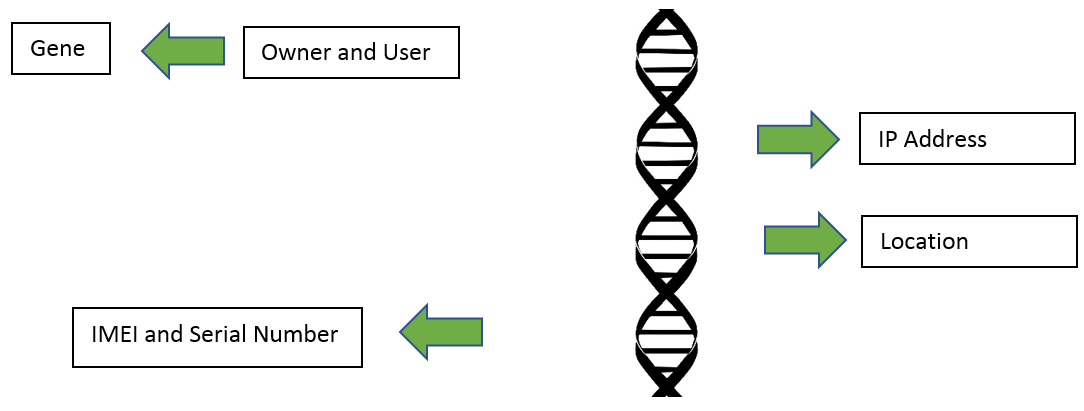
**1.3 Resim Verileri Üzerinden Obje Saptama**

Bu çalışmada, geliştirilmiş olan masaüstü uygulaması yardımıyla bulut ortamına kayıt edilen IoT cihazlarından çekilmiş olan resim verileri üzerinde sınıflandırma işlemi yapılması amaçlanmaktadır. Bu bilgi ışığında, IoT cihazından çekilmiş silah ve bıçak resimlerinin suç işlemeye ihtimal verebilmesi sebebiyle yetkili kurumlara uyarı mesajı gönderilmektedir. Bu işlem için tasarlanmış olan CNN modeli ile birlikte IoT cihazlarından elde edinilen resim verileri birlikte kullanılarak tahmin sonuçlarına göre bir karar mekanizması kurulmuştur. Bu işlem sırasında CNN modelinin eğitilmesi aşamasında silah ve bıçak objeleri için [1 0] etiketi kullanılırken herhangi bir suç objesi içermeyen çiçek resimleri [0 1] etiketi kullanılarak etiketlenmiştir. Bu etiketleme işlemlerine göre gerçekleştirilen model eğitimi ile birlikte objeleri saptayabilen ve buna ek olarak sınıflandırma işlemini gerçekleştiren bir CNN modeli kurulmuştur. Şekil 1.3.1 silah, bıçak ve çiçek objeleri için saptanmış görüntülerin sınıflandırma metodolojisini açıklamaktadır.

Şekil 1.3.1 : Silah, bıçak ve çiçek objelerinin saptanması ve sınıflandırılma işlemleri

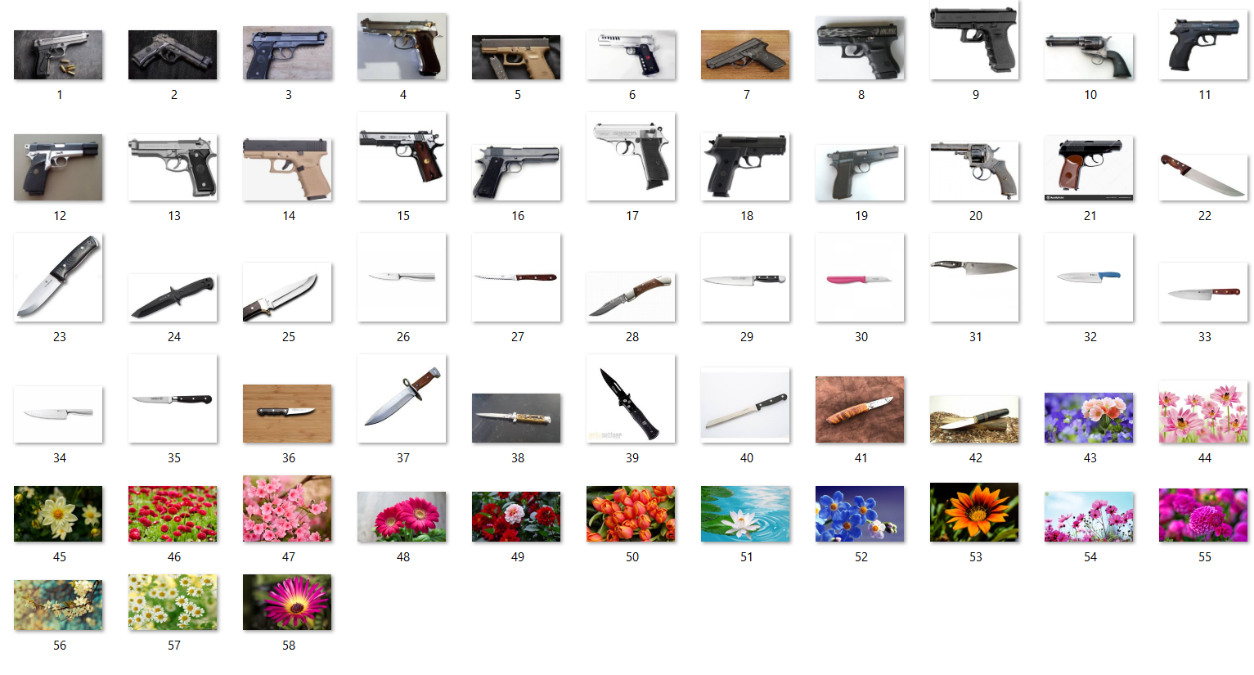
Şekil 1.3.1 ‘ de gösterildiği üzere input verisi olarak kullanılan silah, bıçak ve çiçek resimleri sırasıyla Input, Hidden ve Output katmanlarından geçirilerek işlenir. İşlem tamamlandığında ise üç tip obje iki sınıfa bölünür. Eğer çekilen resim silah veya bıçak objesi ise sinir ağı modeli tarafından saptanır ve masaüstü uygulamasına IoT cihazının soruşturulması için uyarı mesajı gönderilir. Eğer çekilen resim bir çiçek resmi ise bu obje suç teşkil etmediği için IoT cihazının soruşturulması gerekli değildir. Bu açıdan, masaüstü uygulamasına herhangi bir soruşturma uyarısı mesajı gönderilmez.

**1.4 IoT Cihaz Bilgisi Modeli**

Günümüzde hızlıca gelişmekte olan IoT teknolojileri içerisinde barındırdığı cihazlar ile birlikte oldukça fazla sayıda cihaz özelliğini de içerisinde barındırmaktadır. Bu çalışmada ön görülen IoT cihaz modelinde ise DNA sarmalını anımsatan bir model öne sürülmektedir. Buradaki her bir alan DNA içerisinde bulunan gen dizilimini ifade etmektedir. IoT cihazları için temelde sahip adı, kullanıcı adı, IMEI numarası, bağlanılmış olan ağın IP Adresi ve son olarak cihazın anlık konum bilgileri (latitude ve longitude) saklanmaktadır. Şekil 1.4.1 IoT cihazı bilgisi modelini göstermektedir.

Şekil 1.4.1 : IoT cihaz DNA ve Gen modeli

**1.5 IoT Cihazlarından Elde Edilmiş Resim Veri Seti**

Gerçekleştirilmiş olan çalışmanın en önemli parçalarından bir tanesi de veri setidir. Bu çalışmada IoT cihazlarından elde edilmiş olan resim verileri çalışmanın içerisinde bulunan ve karar verme mekanizması olarak çalışan CNN modeline input olarak verilir. Bu çalışma için 58 adet resim öğesiyle eğitilmiş CNN modeli %85 civarında bir tahmin doğruluğu değerine sahiptir. IoT cihazından çekilen resimlerin formatlarının .jpg uzantılı olduğu kabul edilmiş ve CNN modelinin yazılımsal olarak bu resimleri okuyabilmesi için geliştirilen kod dizimi buna göre adapte edilmiştir. Son olarak, veri seti ile CNN modeli %100 uyumlu çalışmaktadır. Herhangi bir runtime veya mantıksal hata meydana gelmemektedir. Resimlerin tahmini işleminde ise her IoT cihazından elde edilmiş ikişer resim üzerinde tahmin işlemleri yapılmaktadır. Toplamda 108 resim üzerinden gerçekleştirilen derin öğrenme süreçleri ile beraber yüksek doğruluk değerine sahip bir CNN modeli oluşturulmuştur.

Şekil 1.5.1 : IoT cihazlarından elde edilmiş veri seti

1. **ÇOKLU SUNUCULAR İÇİN IoT ADLİ BİLİŞİM**

Hemen hemen tüm adli bilişim soruşturma modelleri temel olarak *yetkilendirme , planlama ve izine sahip olma* kavramlarını esas alır. Buna ek olarak, bu kavramlar standart operasyonel prosedürler (Standart Operational Prodecures) olarakta adlandırılır. Bu temel esaslar herhangi bir adli bilişim soruşturmasının temellerini oluşturur ve gelecek işlemler bu temeller üzerine kurulur.

Öngörülen mimari ve çalışmalar inşa edilirken ilk paragrafta yer verilen esasler kabul edilmiştir. Bulut bilişim üzerinde sanallaştırılmış ülke sunucuları ana sunucuları, ülkelerin alt katmanlarında bulunan şehirler ise alt sunucuları oluşturmaktadır. Şehirler üzerinde kurulan alt sunucular bulundukları ülkenin sunucularına bağımlıdır. Sistem üzerinde 6 adet ülke bulunmaktadır. Alt sunucu olarak ise 12 adet şehir ve her şehirde kurulmuş toplamda 12 adet alt sunucu bulunmaktadır. Bu mimari ile IoT cihazları için çoklu sunuculu bir platform tasarlanmıştır. Bulut bilişim ile insan etkileşimini sağlamak amacıyla bir adet çok fonksiyonlu uygulama geliştirilmiştir. Bu kapsamda sistemin paydaşları uygulamayı kullanarak sistem ile etkileşime geçebilirler. Ayrıca geliştirilen uygulama yapılacak soruşturmalar içinde bir etkileşim elemanı olarak kullanılmaktadır.

|  |  |
| --- | --- |
| **Ana Sunucular (Main Servers)** **Alt Sunucular (Sub-Servers)** | |
| **TÜRKİYE (TR)** | Ankara (AN), Istanbul (IS) |
| **BİRLEŞİK KRALLIK (GB)** | Londra (LD), Portsmouth (PT) |
| **ALMANYA (GR)** | Berlin (BE), Köln (CG) |
| **FRANSA (FR)** | Paris (PR), Lyon (LY) |
| **İTALYA (IT)** | Roma (RM), Napoli (NP) |
| **İSPANYA (SP)** | Madrid (MD), Barselona (BC) |

Tablo 2.1 : Ana ve alt sunucuların adları ve kodları. [9]

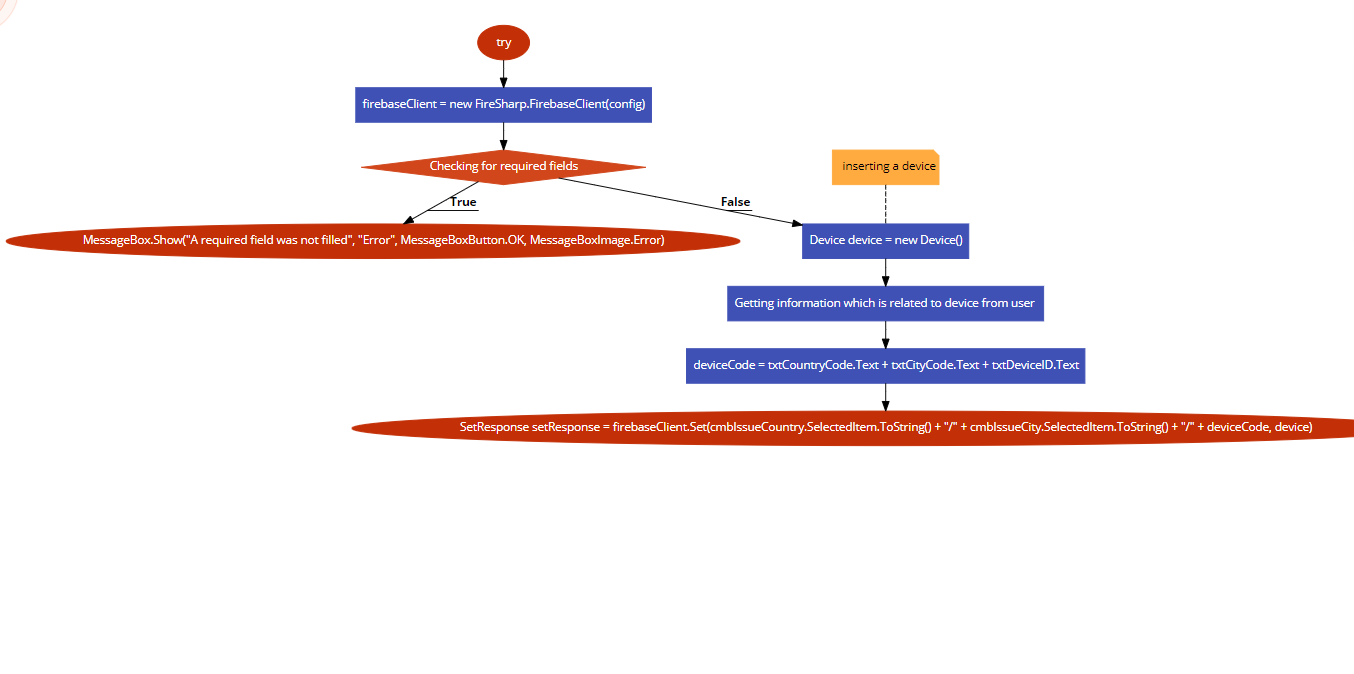
Geliştirilen platform cihaz kullanıcılarına ve soruşturma amirlerine belirli kullanılabilir fonksiyonlar sağlamaktadır. Bunlara örnek olarak, kayıt olma (Registration), cihaz kaydı oluşturma (Device Registration), cihaz takip platformu (Device Trace Platform), cihaz sorgulama (Device Investigation) gibi fonksiyonları barındırmaktadır. Bu bağlamda, sistemle etkileşen bireyler için C# programlama dili kullnılarak Visual Studio 2017 IDE ortamında bir adet uygulama geliştrilmiştir. program inşa edilirken bireylerin sistemi rahat kullanımı ön planda tutulmuştur. Ayrıca proje planlaması sırasında gereksinimler iyi kavranmış, gelecekte yapılacak geliştirmeler ve yatırımlara göre proje planlaması yapılmıştır. Sisteminn çalıştırılması sırasında ilk olarak açılan arayüz yardımıyla kullanıcılar sisteme erişebilirler. Sistemin güvenliği açısından Login işlemi sırasında gerekli kullanıcı kontrolleri yapılmıştır. Sistemle etkileşmek isteyen bir kullanıcının aktif bir hesap bilgisi yoksa sisteme girişi engellenmiş ve uyarı mesajı kullanıcıya döndürülmüştür. Cihazları kayıt etmek için hesap oluşturma hakkı yetkili makamlara aittir. Bu bağlamda, bulut platform üzerinde kayıtlı her bir kişisel hesap sisteme bağlanabilir ve cihaz kayıt edebilir. Sisteme kayıt edilen cihazlar bulut platform üzerinde kayıt ediliği ülke ve şehire göre depolanmaktadır. Alınmış olan ülke ve şehir bilgisine göre ana sunucuya kayıt işlemi gerçekleştirilmektedir.

**2.1 IoT Cihaz Kaydı Oluşturma (Registration)**

Öngörülen mimarinin ilk ve en temel adımı bulut platforma arayüz yardımıyla cihaz kayıt etmektir. Buna göre sisteme bağlanan kullanıcılar kayıt etmek zorunda oldukları bilgiler ile beraber bulut platformu olarak kullanılmış olan Firebase platformuna verilerini aktarıp IoT cihazlarını kullanabilirler. Bu işlem sırasında bölüm 1’de bahsi geçen merdiven modeli kullanılmaktadır. Şekil 2.1.1 merdiven modelinin ayrıntılı gösterimidir.

|  |  |
| --- | --- |
| CİHAZ bilgileri | AÇIKLAMA |
| sahip (OWNER) | IoT cihazını satın alıp sisteme kayıt ettiren kişiyi temsil etmektedir. |
| Kullanıcı (USER) | IoT cihazını aktif olarak kullanan kişiyi temsil etmektedir. |
| IMEI NUMARASI (IMEI NUMBER), SERİ NUMARASI (SERIAL NUMBER) | Kullanımda olan cihazın eşsiz olan IMEI ve Seri numaralarını temsil etmektedirler. |
| Lokasyon(LOCATıON) (LATITUDE AND LONGITUDE ) | Cihazların anlık konumunun takibi için gerekli enlem ve boylam bilgisidir. Kayıt işlemi sırasında otomatik olarak cihaz üzerinden çekilir. |
| IP Adresi (IP ADDRESS) | Cihazın bağlı olduğu ağın IP adresini temsil etmektedir. |

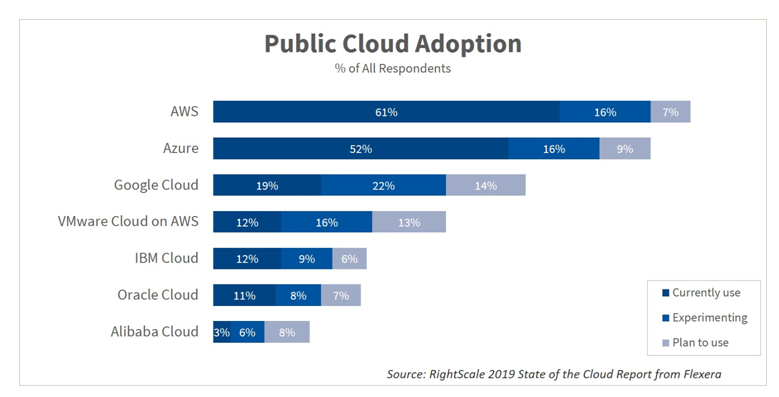
Tablo 2.1.1 : IoT cihazlarının sisteme kayıt edilmesi sırasında cihazların taşıdığı bileşenleri (DNA Modeli) göstermektedir. [10]



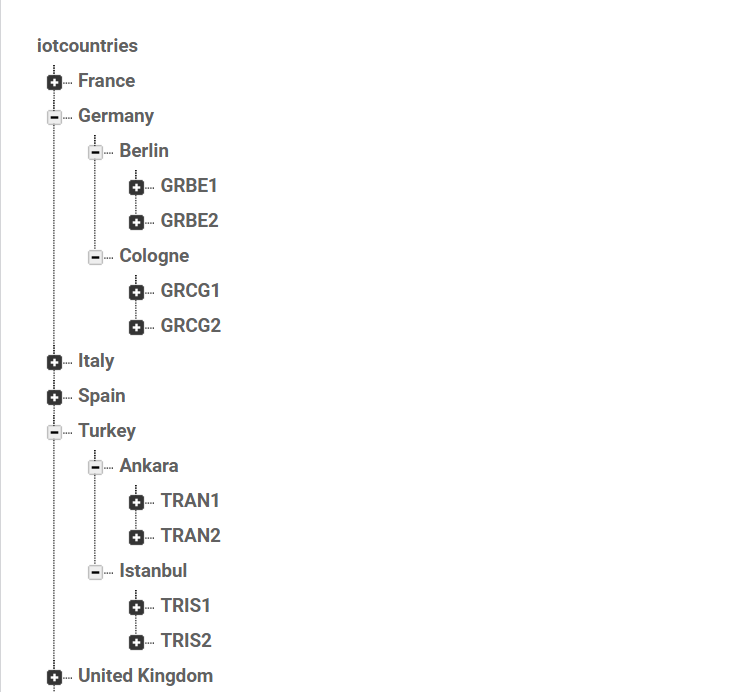
Tablo 2.1.2 : IoT cihazının masaüstü uygulaması ile bulut ortamına kayıt edilmesi

**2.2 Bulut Platformu (Firebase)**

Günümüz IoT teknolojilerinin en önemli bileşenlerinden birisi de bulut platformlarıdır. Bir çok bulut mimarisi bu teknoloji alanında kullanılmaktadır. Yapılan araştırmlara sonucunda varılan sonuçlara göre birçok bulut platformunun IoT projelerinde kullanıldığı anlaşılmaktadır. Bunlara örnek olarak Amazon Web Services, Microsoft Azure, Google Cloud (Firebase), IBM Cloud ve Oracle Cloud verilebilir. Bu platformlardan bazıları ücretsiz kullanıma izin verirken, bazılarıda ücretli kullanımla hizmet vermektedir. Son yıllarda üzerinde olan ilgiyi artıran bulut platformlar kullanıcılarına kullanışlı imkanlar sunmaktadır. Veritabanlarına yazılmış veriler üzerinde analizler yaparak, kullanıcılarına yapılan analizler sonucunda oluşan veri sonuçlarını sunmaktadır. Bunlara ek olarak, gerekli güvenlik önlemleri de bazı bulut platformlarının kurulu sırasında kendi içlerinde bulunmaktadır. Her geçen gün hızla büyüyen bu sektör ilerleyen yıllarda daha büyük ivme ile büyüyeceği uzmanlar tarafından tahmin edilmektedir.



Şekil 2.2.1: Günümüz Bulut Platform Kullanım Bilgileri [11]

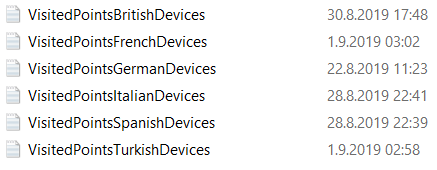
Yazılım mimarisi tasarlanırken her proje başlangıcında olduğu gibi yapının performansı için en iyisi seçilmesi düşünülmüştür. Bu kapsamda kullanılan Google Cloud Firebase platformu öngörülen mimariyle kullanılması en makul olandır. Firebase kullanıcılarına real-time ve cloud firestore olmak üzere 2 seçenek sunmaktadır. Bu çalışmada, verilerin saklanması için real-time veritabanı kulanılmıştır. Buna ek olarak, Google tarafından sunulan bu imkanın ücretsiz olması sistemin geliştirme maliyetini düşürmüştür.

Şekil 2.2.2 : Bulut Platform mimarisi [12]

Bir önceki bölümde belirtilen cihaz kayıt işleminin başarılı bir şekilde gerçekleştirilmesinin ardından, arayüze girilmiş bilgiler Firebase’e başarılı bir şekilde kaydedilir. Firebase mimarisi şekil 2.2.1’de şematize edilmiştir. Kullanıcıdan alınmış gerekli bilgiler bulut ortamında mantıksal gereksinimler dogrultusunda depolanmaktadır. Cihazların sahip olduğu bilgiler gerekli olduğu durumlarda bulut ortamından dış dünyaya sunulabilmektedir. Şekil 2.2.1’de bulut platformunun mimarisi ve cihaz dağılımı gösterilmektedir.

Şekil 2.2.1’den de kolaylıkla anlaşılabileği üzere kullanıcı arayüzü yardımıyla kayıtları yapılan cihazlar ülke, şehir ve sıra numarası kodlarıyla oluşturulmuş evrensel kimlik numaralarına göre kayıt edildikleri şehir ve ülkelere göre bulut ortamına kayıt edilmektedir. Her bir cihazın taşıdığı cihaz bilgileri bulut platformu üzerinde görülebilmektedir. Bu bilgiler talep edildiği takdirde uygulamanın diğer fonksiyonlarına sunulmaktadır.

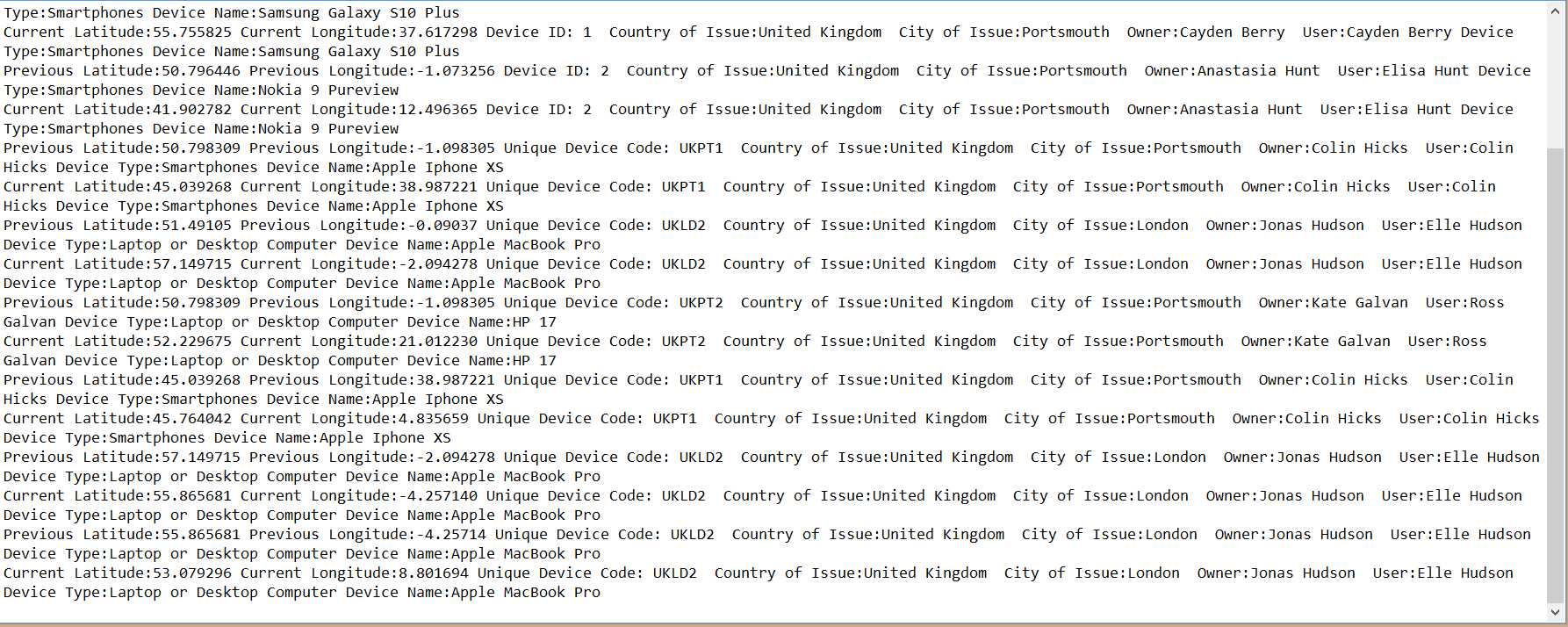
**2.3 IoT Cihaz Takip ve Haritalama Algoritmaları**

Gelişmekte olan nesnelerin interneti alanında lokasyona göre cihaz takibi başı çeken konulardan biridir. Temelde, aldığı enlem ve boylam bilgisine göre kullanımda olan cihazın anlık lokasyonunu bağlı olarak çalışan bir işlemdir. Forensik alanında lokasyon bilgisi geçmişi, haritalama ve cihaz takibi gibi uygulamalar çok önemli konulardandır. Bununla ilişkisel olarak, tasarlanmış uygulama da cihazların takibinin ve anlık lokasyonlarının yapılabileceği bir haritalama arayüzü tasarlanmış. Uygulamanın çalışması sırasında soruşturma amirleri tarafından verilen talimat geregince cihazların oldukları anlık lokasyon harita üzerinde gösterilmektedir. Haritalama algoritmalarının oluşturulması sırasında Google Maps in C# üzerinde çalıştırılması ile probleme çözüm üretilmiştir. Anlık lokasyon bilgisinin harita üzerinde gösterimi sırasında, geliştirilen uygulama ile bulut platform arasında senkron çalışan bir köprü kurulmuştur. Cihazın anlık yer degiştirmeleri bulut platformuna dogrudan yansıyacağından, cihazın sürekli hareketi haritalama algoritmalarının çalışmasını olumsuz anlamda etkilemeyecektir. Buna ek olarak, cihazların yaptıkları lokasyon değişikliklerini dosyalarda saklamak, gelecekte yapılacak soruşturmalar için hayati önem taşımaktadır. Bu yaklaşımdan yola çıkarak, uygulamanın kurulduğu bilgisayarlarda cihazların lokasyon değişikliklerini gözlemleyebilmek için ülke adlarına göre açılmış dosyalar bulunmaktadır. Bu dosyaların içerisinde bulunduğu ülkeye kayıtlı cihazların lokasyon değişiklikleri bulunmaktadır. Cihazların anlık hareketleri hem bulut platformuna hemde bu dosyalara kayıt edilmektedir. Bu veriler bir cihazın ileride geçireceği herhangi bir soruşturma için önemli birer delil niteliğindedirler. Bu açıdan, bu dosyaların korunması ve dışarıdan sisteme erişmiş kötü niyetli paydaşlardan tarafından değiştirilmemesi oldukça önemlidir. Herhangi bir bir değişiklik durumu cihaz üzerinde yapılacak soruşturmayı direk etkileyeceği için bu dosyalar şifrelenmiştir. Bu dosyalara erişim hakları sadece yetkili paydaşlara verilmiştir. Fakat, yetkililerin bu dosyalara erişmesi demek dosyaları değiştirebileceği anlamına gelmemektedir. Bu dosyalar üzerinde yapılacak herhangi bir değişiklik kötü sonuçlar doğurabileceği için yetkililere sadece okuma işlemi yaptırılmaktadır. Güvenlik gerekçelerinden ötürü yazma işlemi yapılmamalıdır. Şekil 2.3.1 uygulama üzerindeki haritalama algoritmalarının çalışmasını, şekil 2.3.2 ise lokasyon değişikliklerinin kayıt edildiği dosyaların görünümünü temsil etmektedir.

Şekil 2.3.1 : IoT cihazlarının lokasyon değişikliklerinin tutulduğu özel dosyalar.

Şekil 2.3.2 : IoT cihazlarının anlık lokasyonuna göre harita üzerinde gösterilmesi. [13]

Şekil 2.3.2’de yapılan uygulama üzeriden bir yorum yapılırsa, soruşturma amirleri kayıtlı ülke, şehir ve cihaz kimliği bilgileriyle cihazları takip edebilirler. Cihazlar kayıtlı oldukları ülkelerin bayrakları ile temsil edilmektedir. Buna ek olarak cihazların konum değişikliğinde önceki konumları harita üzerinden silinmez. Böylelikle kullanıcıların takip ettikleri yollar kolaylıkla belirlenebilir.

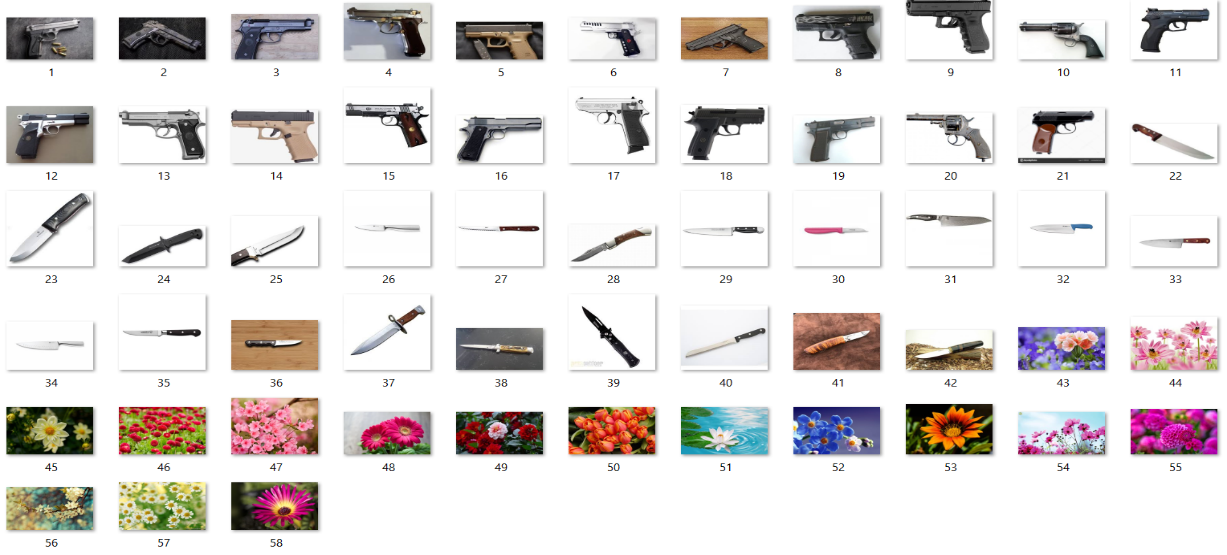
Yukarıdaki görselde belirtilmiş dosyalar kod mimarisinin içerisine gömülü olarak bulunmaktadır. Cihazın lokasyonu değiştiği anda kayıtlı olduğu ülkeye göre lokasyonunda olan değişiklik cihaz bilgileri ile birlikte dosyalara yazılmaktadır. Cihazların özellikleri ile lokasyon değişiklik bilgileri şekil 2.2.3’de gösterilmiştir.

Şekil 2.3.3 : Cihazların lokasyon değişikliği sırasında dosyaların içerik durumu.

Şekil 2.3.3 üzerinde de görüldüğü gibi herhangi bir cihazın konumu değiştiği an, o andaki cihazın önceki ve anlık lokasyonu, cihaz kodu, kayıtlı olduğu ülke ve şehir, sahip ve kullanıcı isimleri ve cihaz ismi ile cihaz tipi dosyalara yazdırılır. Böylelikle konumu değişen cihazların kapsamlı bilgileri sistemi kontrol eden soruşturma amirlerine sunulacak duruma gelmiştir.

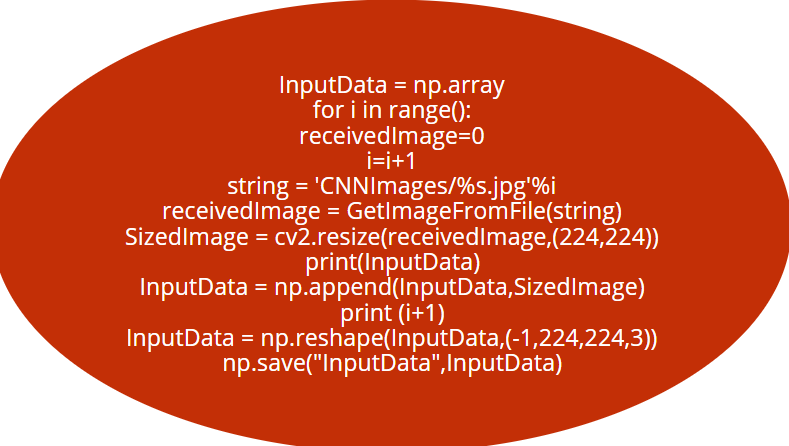
**2.4 IoT Cihazlarındaki Resimlerin CNN Modeline Aktarımı (Preprocessing)**

Kullanıcılar satın aldıkları cihazları masaüstü uygulaması yardımıyla sisteme kayıt ettikten sonra her cihaz için delillerin toplanacağı veritabanına evrensel kimlikleri ile tanımlanan bir alana kaydolurlar. Bu alan içerisine IoT cihazlarından çekilmiş her bir fotoğraf için veritabanı içerisinde kayıt edildiği sunucudaki yerel dosya yolunu barındıran bir alan bulunmaktadır. Bu alanlarda tutulan resimler evrişimsel sinir ağı modelinin giriş (input) verisini oluşturmaktadır. Sunucu üzerinde bulunan tüm IoT cihazından elde edilmiş resim verileri Pyhton programlama dili yardımıyla bir dizi (array) ye alınarak saklanır. Bu işlem sırasında, sunucu üzerinden alınmış her bir resim için yeniden şekillendirme (reshape) işlemi uygulanır. Bu işlemin yapılmasında ki temel esas IoT cihazlarından çekilmiş olan her bir resmin aynı boyutta olamayacağı gerçeğidir. Bu bilginin ışığında işlenecek olan her bir resim öğesi 224x224 lük boyutta ölçeklendirilerek sinir ağı modelinin eğitilmesinde ve test edilmesinde kullanılır. Bu işlem kullanılmış olan resim veri seti için bir ön işleme (preprocessing) niteliği taşımaktadır. Sinir ağı modeli üzerinde işlenecek olan resimler bu işlem sayesinde belirli bir standarta uygun hale getirilir ve modelin ilerleyen safhalarında kullanılmak üzere gerekli diziler de tutulurlar.

Son olarak, IoT cihazlarından elde edilmiş olan resim verilerine yeni eklenen elemanlar olduğunda Pyhton programlama dili yardımıyla yazılmış olan veriduzenlemesi.py dosyası üzerinde teker teker ön işleme fazından geçirilerek sunucuya kaydedilirler. Böylelikle, IoT cihazlarından gelen resim verileri artsa dahi önceden saklanan resimler için tekrar bir ön işleme işlemi gerçekleşmez ve tasarlanmış olan mimari tekrar tekrar çağırılmadığı için yazılmış olan talebi konusunda herhangi bir yoğunluk yaşanmaz. Eğitilecek olan model içerisinde resim öğelerini barındıran bu diziyi kullanarak kendini eğitir ve test, tahmin gibi işlemler için kendisini hazırlamış olur.

Şekil 2.4.1 : IoT cihazlarından elde edilmiş resim öğeleri.

Bu çalışmada uygulanmış olan sınıflandırma işlemi ile birlikte modelin eğitilmesi sonucunda IoT cihazlarından çekilmiş silah, bıçak ve çicek öğeleri ayırt edilebilmektedir.

****

Şekil 2.4.2 : Ön işleme (Preprocessing) mekanizmasının yazılımsal ifadesi.

**3. EVRİŞİMSEL SİNİR AĞI MODELİ KULLANILARAK IOT CİHAZLARINDAN SUÇ TESPİTİNİN GERÇEKLEŞTİRİLMESİ (DERİN ÖĞRENME OPTİMİZASYONU)**

Özellikle son birkaç yıldır popülerleşmeye başlayan konulardan biriside hiç şüphesiz makine öğrenmesidir (ML) . Bahsedilen bu konuyla beraber Yapay Zeka (AI) , Derin Öğrenme (DL) gibi konularda gündeme gelmektedir. Makine öğrenmesinin yapay zekanın alt kümesi olduğu söylenebilir.

ML

AI

DL

Şekil 3.1 : Makine Öğrenmesi, Yapay Zeka ve Derin Öğrenme arasındaki ilişki. [14]

ML için bir tanım yapmak gerekirse, matematiksel ve istatistiksel veriler üzerinden tahminler yapılarak varılan sonuçların bilgisayar ortamında gösterilmesidir. ML’nin günümüzde popülerliğini korumasında en büyük etmen olarak büyük veri bilimi söylenebilir. Buna ek olarak, derin öğrenmenin ise bir makine öğrenimi yöntemi olduğu bilinir. Bu temel bakış açısı baz alınarak, IoT cihazlarından toplanmış resim verileri üzerinde derin öğrenme teknikleri kullanılarak suç tespitinin yapılması amaçlanmaktadır. Bölüm 1’de bahsedildiği gibi IoT teknolojileri ile büyük veri biliminin her geçen arasındaki ilişki gelişmektedir. Makine Öğrenmesi teknikleri kullanılarak, büyük veriler işlenebilir, sonuçlar üretilebilir ve üretilen sonuçlar bir karar mekanizması oluşturulabilir. Bu bölümde ML algoritmalarından bahsedilecek olup, ilişkisel çalışmalar açıklanacaktır. Temel bazda, ML algoritmaları mantıksal ve cebirsel işlemler üzerine kurulmaktadır. Bunlara örnek olarak, Gözetimli (Supervised), Gözetimsiz (Unsupervised) ve Takviyeli (Reinforcement) metodolojilerden bahsetmek mümkündür.

**3.1. Makine Öğrenmesi Metodolojileri**

**Gözetimli (Supervised) :** Bu öğrenme tekniğinde giriş değerleri ile çıkış değerleri arasında eşleme yapan bir sistem kurulur. Classification (Sınıfandırma) ve Regression (Regresyon) algoritmaları yoğun bir biçimde kullanılır.

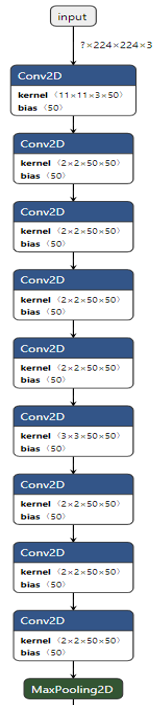
**Gözetimsiz (Unsupervised) :** Gözetimli tekniğin aksine işaretlenmemiş bir veri topluluğu üzerinden sonuç çıkarmaya çalışan bir öğrenim tekniğidir.

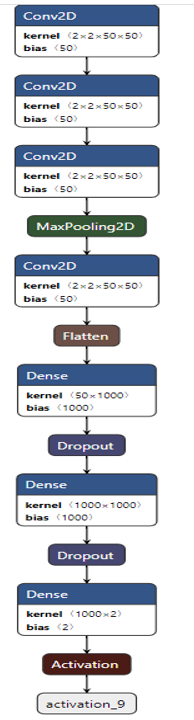
**Takviyeli (Reinforcement) :** Diğer iki teknikten bazı konularda farklılaşmaktadır. Çevreden topladığı verilerden ürettiği sonuçta en iyi skorlu olan sonuca ulaşmayı hedefler

Şekil 3.1.1 ML çatısı altındaki öğrenim tekniklerini gösterimidir. [15]

**3.2 Evrişimli Sinir Ağı Modeli (CNN) (Derin Öğrenme)**

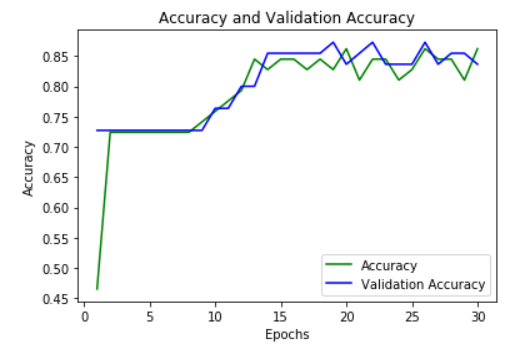
Bölüm 1’de bahsedildiği üzere IoT cihazlarından toplanmış ve delil olma potansiyeline sahip veriler (resim, eposta, görüşme kayıtları, kredi kartı bilgileri vb.) üzerinde Makine Öğrenmesine bağlı olarak dizayn edilen Sinir Ağı Modeli ile suç tespiti yapılması gerçekleştirilmektedir. Spesifik olarak, cihazlardan çekilmiş resimler üzerinde yürütülecek algoritmalar vasıtasıyla bu sonuçlara ulaşılmaktadır. IoT cihazlarından çekilmiş her bir resim bulut platformu üzerinde bulunan *Deliller* veritabanında saklanmaktadır. Buradaki verilerin her bir cihaz için ülke kodu, şehir kodu ve cihaz sıra numaralarına göre oluşturulmuş dosyalar içerisinde saklanmaktadır. Bu dosyalar içerisinde depolanan resim verileri CNN modeli ile optimize olarak çalışarak derin öğrenme tekniklerini işletmektedir. Buradaki işlem üç safhadan oluşmaktadır. Birinci safha, sunucu üzerinde saklanmış olan resimlerin CNN modeline input olarak verilmesi için gerekli olan ön işleme safhasıdır. Bu aşamada, IoT cihazlarından elde edilen resimler standart bir boyutlandırma işlemi geçirir. İşlenecek olan her bir resim önceki boyutu ne olursa olsun CNN modelinin kabul ettiği 224x224 lük bir kare boyutuna çevrilir ve Pyhton programlama dili üzerinden yazılmış olan veriduzenlemesi.py dosyası içerisinde ön işleme tabii tutulmuş resimler ilerleyen safhalarda modelin eğitilmesi için bir dizide saklanır. Ön işlem aşamasının tamamlanmasının ardından ikinci aşama olan CNN modelinin kurulması ve eğitilmesi aşaması başlar. Bu aşamanın başlangıç adımında, ön işlem görmüş resim verilerine etiketleme işlemi yapılır. Bu işlem aracılığıyla, silah ve bıçak resimleri için [ 1 0 ] etiketi, çiçek resimleri için [0 1] etiketi atanmıştır. Bu işlemin amacı, CNN modelinin eğitimi sırasındaki öğrenme işleminin gerçekleşmesi içindir. Etiketlenmiş veriler modele input olarak verildikten sonra özellik çıkarımının yapılması için CNN modelinin iç yapısının içerisine girer. Burada sırasıyla convolution, pooling, convolution, pooling katmanlarından geçtikten sonra etiketlenmiş resimler için özellik çıkarımı safhası tamamlanmış olur. CNN modelinin ikinci fazında ise sınıflandırma işlemi başlar. Özellik çıkarımı işleminden geçirilen tüm veriler ilk olarak flatten tabakasından geçirilir. Bu işi takip eden dense ve activation katmanları ile beraber resimler outpu layer aracılığıyla iki sınıfa bölünmüş olur ve öğrenme işlemi tamamlanır. CNN modelinin bu döngüyü 30 epoch tekrarladığı bilinmelidir. 30 epoch çalıştırılan model sonucunda modelin kendi verilerinden öğrenme yüzdesi %84.48 dir. İlk defa göreceği resim öğelerinde ise doğruluk oranı %87.27 dir. Özetle optimize edilmiş derin öğrenme ve CNN modeli yüksek doğruluk oranı ile çalışmaktadır. Şekil 3.2.1 CNN modelinin yapısını, şekil 3.2.2 ise optimize edilmiş olan CNN modelinin accuracy ve val\_accuracy değerlerinin 30 Epochs süresince değişimini göstermektedir.





Şekil 3.2.1 : CNN modelinin katman yapısı

Şekil 3.2.1’ de gösterildiği üzere, sol taraftaki birinci görsel CNN modelinin özellik çıkarım mekanizmasının büyük bir kısmını göstermektedir. Sağ taraftaki ikinci görselde ise sınıflandırma katmanında görev yapan metodlar görünmektedir. Kurulmuş olan çalıştırılıp sunucu üzerinde kayıt edilerek diğer işlemler için tekrar tekrar çağırılmaya gerek duymadan çalıştırılmaktadır. Genel olarak kurulan model tutarlı çalışıp doğru sonuçlar üretmektedir. İlk etapta kayıt edilen 25 IoT cihazı için sadece bir cihazda yanlış tahmin yapmaktadır.

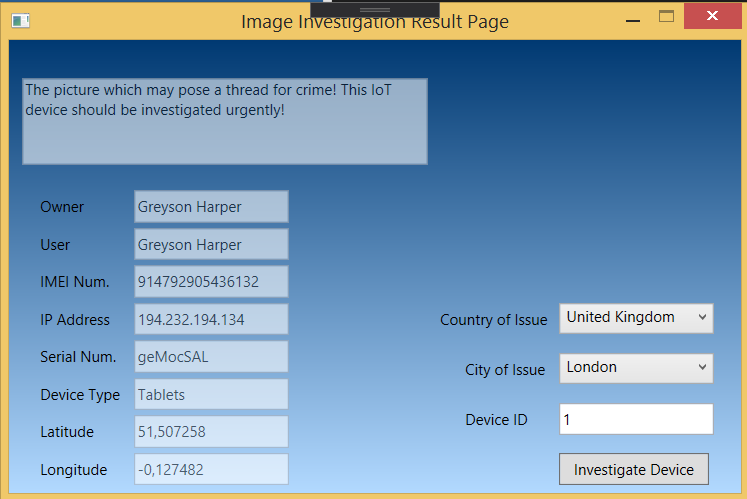
CNN modelinin üçüncü safhası ise tahmin yapma aşamasıdır. Eğitilmiş model üzerinde gerçekleştirilen tahmin işlemleri sonucunda yüksek doğruluk oranı yakalanmıştır. Şüpheli bulunan cihazların soruşturma uyarısı mesajları masaüstü uygulaması ile optimize çalışarak sonuçlar yetkili kişilere gösterilmektedir.

Şekil 3.2.2 : CNN modelinin Epoch sayısına göre doğruluk yüzdesi grafiği

**3.3 IoT Cihazlarından Toplanmış Resimler Üzerinde CNN Modeli İle Sonuç Çıkarımı**

3.2 numaralı bölümde de belirtildiği gibi CNN modeli temelde veri düzenlemesi, eğitim ve tahmin olmak üzere üç aşamadan oluşmaktadır. Bu aşamalardan üçüncüsü ise IoT cihazlarından elde edilmiş olan resimler üzerindeki tahmin işlemidir. Bu aşama ile beraber eğitilmiş CNN modeli üzerinde input olarak verilen test verilerinin aracılığıyla giriş resimlerinin tahmininin yapılması sağlanır. Bu işlem sonucunda yüksek bir başarı oranı yakalanmıştır. Böylelikle IoT cihazlarından eklenecek olan resimlerin soruşturmaları daha hızlı şekilde sürdürülüp resimler üzerinden herhangi bir suç teşkil edip etmediği kolaylıkla belirlenebilecektir.

**3.4 Saptanmış Objelerin Sonuçlarının Bildirimi**

CNN modeli üzerinden gerçekleştirilen tahmin sonuçlarının masaüstü uygulamasına döndürülmesi gerçekleştirilmiştir. Bu safhada, her bir IoT cihazı için oluşturulan .txt dosyaları içerisine tahmin sonuçları [1 0] ve [0 1] olarak yazdırılmaktadır. Önceki bölümlerde de anlatıldığı üzere bu safhada [1 0] etiketi suç teşkil edebilen cihazlar için kullanılan etiket türüdür. [0 1] etiketi ise yasadışı herhangi bir problem yaratmayacak resimler için atanmış etikettir. CNN modeli üzerinden dönen sonuçlar her bir cihaz için sunucuda açılmış olan .txt dosyasına yazılırlar. Bu yazılma işlemi tamamlandıktan sonra masaüstü uygulama için geliştirilmiş olan kodlar vasıtasıyla her bir cihaz için oluşturulan bu dosyalar satır satır okunur ve herhangi bir [1 0] etiketine rastlanırsa bunun suça ihtimal verebileceği göz önüne alınarak yetkili kişilere sonuçlar bildirilir. Eğer cihaz içerisinde herhangi bir suça karışabilecek bir obje yok ise kullanıcın bilgileri kişisel veri gizliliği esas alınarak yetkili kişilere gösterilmez.

Şekil 3.4.1 IoT cihazındaki obje tespitinin sonucunun bildirimi

Şekil 3.4.1 de görüldüğü üzere Birleşik Krallık / Londra merkezli 1 numaralı cihaz içerisinde suç işlemeye ihtimal verebilecek belli öğelerin olduğu tespit edilmiştir. Bu tespitin ardından IoT cihazının soruşturulma uyarısı yetkili kişi ve kurumlara masaüstü uygulaması yardımıyla bildirilmektedir.

**4. İLGİLİ ÇALIŞMALAR**

Günümüz çağında yeni teknolojiler üzerinde birçok çalışma yürütülmektedir. Nesnelerin internetide bu yeni gelişmekte olan alanlardan biridir. 2000’li yıllarında başlayan RFID teknolojileri ile adını ilk defa duyuran IoT, geçtiğimiz özellikle son 10 yılda hızla gelişmektedir. Çalışma konumuz olan Forensik IoT ise merkez olarak İngiltere ve Amerika menşeiyli üniversitelerde yapılan araştırmalarda adını duyurmuştur. İngilterede birçok üniversitede kriminoloji ve bilgisayar bilimleri departmanları ortak çalışmalar yürütmektedir. Buna ek olarak, özellikle Avrupa Birliğine üye ülkelerin hükümetleri artan siber suçlar üzerine ülkelerindeki sanayi kuruluşlarına gerekli güvenlik önlemlerini almaları için teşviklerde bulunmaktadır. Son yıllarda adını sıkca duyuran siber güvenlik, IoT forensik ve diğer güvenlik konularıyla dogrudan ilişkili olduğu söylenebilir. [17]

**5. DENEYSEL ÇALIŞMALAR VE SONUÇLAR**

Özetle, bu çalışmanın amacı gelişmekte olan bilgisayar bilimleri ve bunun parallelinde mesafe kat eden teknolojik cihazların daha güvenilir bir ortamda kullanılmasını sağlamaktır. Bu kapsamda öngörülen sistemde sanallaştırılmış ana ve alt sunucular üzerinde kayıtlı olan cihazların sisteme tanınması, kimliklendirilmesi, lokasyonuna bağlı olarak takip edilmesi ve sağladıkları verilerin delil potansiyeli kapsamında saklanması hedeflenmektedir. Son yıllarda kullanımı ve üzerinde yapılan araştırma sayısının oldukça arttığı büyük veri biliminden de yararlanılarak elde edilmiş verilerden suç teşkil edebilecek onlanları ayırt etmek diğer bir hedeftir. Bu kapsamda IoT, Makine Öğrenmesi ve Büyük Veri bilimlerinin bir arada kullanılması sonucunda IoT cihazlarından elde edilen resim verileri üzerinde işletilen algoritma ve CNN modeli ile birlikte IoT cihazındaki resimlerden suç oluşturabilme potansiyeli olanlar tespit edilmiştir. Herhangi bir IoT cihazında karşılaşılan suç aleti durumunda, yetkili soruşturma amirlerine bildirim yapılarak olayın aydınlatılması için çaba harcanacaktır. Bu işlemin gerçekleştirimi sırasında %85 oranında bir doğruluk oranı yakalanmıştır. Bunula beraber kullanımı artan akıllı cihaz alanında daha güvenilir teknolojilerin kullanıcılara sunulması amaçlanmaktadır. Gelecek çalışmalar ise bu mentalite üzerine kurulup, derin öğrenme ile optimize edilen CNN modeli üzerinden farklı veri tipleri için suç tespitinin yapılabilmesidir.[18]

**6. KAYNAKLAR**

[1] A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective Shanzhi Chen, Senior Member, IEEE, Hui Xu, Dake Liu, Senior Member, IEEE, Bo Hu, and Hucheng Wang IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 4, AUGUST 2014

[2] IoT Device Forensics and Data Reduction DARREN QUICK1 AND KIM-KWANG RAYMOND CHOO 1,2, (Senior Member, IEEE) 1 School of Information Technology & Mathematical Sciences, University of South Australia, Adelaide, SA 5001, Australia 2 Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249, USA

[3] Áine MacDermott, Thar Baker, Qi Shi, IoT Forensics: Challenges For The IoA Era, 978-1-5386-3662-6/18/$31.00 ©2018 IEEE Conference Paper · February 2018

[4] Áine MacDermott, Thar Baker, Qi Shi, IoT Forensics: Challenges For The IoA Era, 978-1-5386-3662-6/18/$31.00 ©2018 IEEE

[5] Received November 11, 2019, accepted November 25, 2019, date of publication November 28, 2019, date of current version December 12, 2019. Digital Object Identifier 10.1109/ACCESS.2019.2956681 High-Speed Searching Target Data Traces Based on Statistical Sampling for Digital Forensics DOOWON JEONG AND SANGJIN LEE Digital Forensics Research Center, Korea University, Seoul 02841, South Korea

[6-7]Sundresan Perumal, Norita Md Norwawi, Valliappan Raman, Internet Of Things(IoT) Digital Forensic Investigation Model: Top-Down Forensic Approach Methodology ISBN: 978-1-4673-6832-2©2015 IEEE

[8] Edewede Oriwoh, David Jazani, Gregory Epiphaniou, Paul Sant, Internet of Things Forensics: Challenges and Approach 2013 ICST

[9-10-12] [https://firebase.google.com/docs/database /](https://firebase.google.com/docs/database%20/)YasinEmirKutlu

[11]<https://medium.com/@kursataelf/en-i%CC%87yi-bulut-bili%C5%9Fim-platformlar%C4%B1-kar%C5%9F%C4%B1la%C5%9Ft%C4%B1rmas%C4%B1-ce8383cd638b>

[13][https://github.com/yasinemirkutlu44/Forensics-for-IoT-Multiple Servers/blob/master/Forensic/MapWindow.xaml.cs](https://github.com/yasinemirkutlu44/Forensics-for-IoT-Multiple%20Servers/blob/master/Forensic/MapWindow.xaml.cs)

[14-15]<https://medium.com/t%C3%BCrkiye/makine-%C3%B6%C4%9Frenmesi-nedir-20dee450b56e>

[16] AUGUSTO J. V. NETO, JOEL J. P. C. RODRIGUES, HUGO BARROS CAMBOIM, TORSTEN BRAUN , Fog-Based Crime-Assistance in Smart

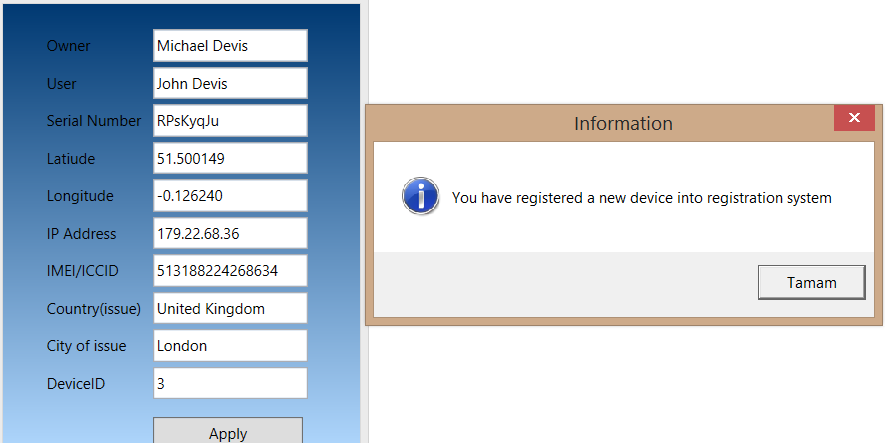
IoT Transportation System, Digital Object Identifier 10.1109/ACCESS.2018.2803439, date of publication February 7, 2018,

[17] Victor R. Kebande, Indrakshi Ray, A Generic Digital Forensic Investigation Framework for Internet of Things(IoT), 2016 IEEE 4th International Conference on Future Internet of Things and Cloud

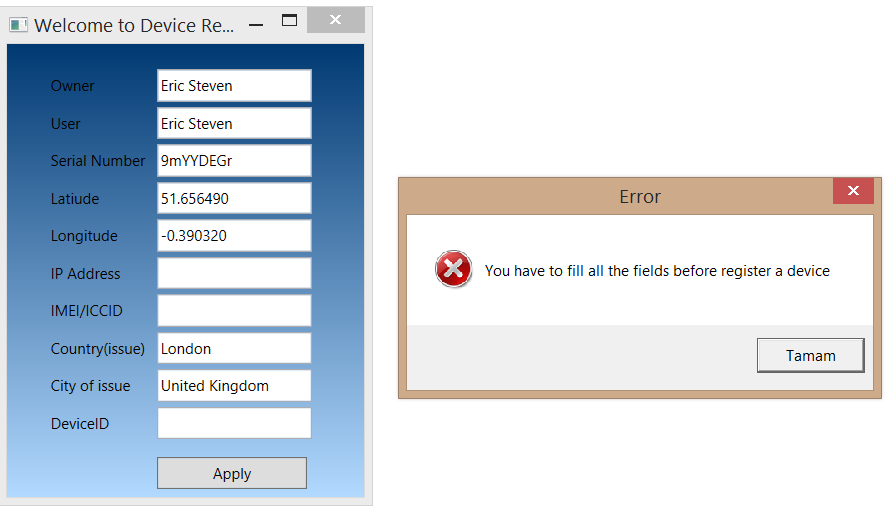
[18] Mr.P.Leninpugalhanthi (ASST PROF), Janani.R, Nidheesh.s, Mamtha R.V, Keerthana .I, Mr R.Senthil Kumar (ASST PROF), Power Theft Identification System Using Iot 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS 2019)

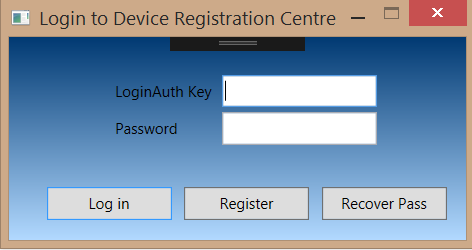
**Proje Kaynak Kodları, Bitirme Tezi, Sunum için GitHub linki :** [**https://github.com/yasinemirkutlu44/Forensics-for-IoT-Multiple-Servers**](https://github.com/yasinemirkutlu44/Forensics-for-IoT-Multiple-Servers)

**7.EKLER**

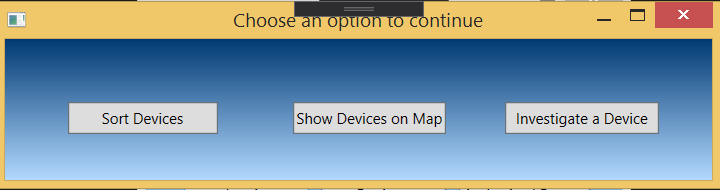
Bu bölümde geliştirilmiş olan uygulamanın ekran çıktıları bulunmaktadır.

Şekil 7.1 : IoT Cihaz kayıt işlemi

Şekil 7.2 : Başarısız cihaz kayıt işlemi hata mesajı



Şekil 7.3 : Login penceresi

Şekil 7.4 : IoT cihaz soruşturma penceresi



Şekil 7.5 : IoT cihaz soruşturma sonuç bildirimi

Öğrenci : Yasin Emir Kutlu

Okul No : 150202040

İmza :