1001 – BİLİMSEL VE TEKNOLOJİK ARAŞTIRMA PROJELERİNİ DESTEKLEME PROGRAMI

PROJE BAŞVURU FORMU

Proje Başlığı: *Kritik Altyapılar İçin Federe Öğrenme Çerçevesinde Çok Amaçlı Şifreleme Optimizasyonu*
Proje Yürütücüsü: Doç. Dr. Oğuzhan Ceylan
Projenin Yürütüleceği Kurum/Kuruluş: Kadir Has Üniversitesi

ÖZET

Proje Özeti

Enerji, ulaşım, haberleşme ve sağlık hizmetleri gibi **kritik altyapılar (KA)**, hem **ulusal güvenlik** hem de **toplumsal refah** için yaşamsal öneme sahiptir. Bu altyapılarda kullanılan **Endüstriyel Kontrol Sistemleri (EKS)** ve **Nesnelerin İnterneti (IoT)** cihazları, genellikle **düşük işlem gücü**, **sınırlı enerji kapasitesi** ve **kısıtlı ağ bant genişliği** gibi kısıtlarla çalışmaktadır. Bu durum, **geleneksel merkezi yapay zekâ çözümlerini** uygulanamaz hale getirmektedir. Bu bağlamda, **Federe Öğrenme (FL)**; **veri gizliliği**, **düşük gecikme**, ve **yerel model eğitimi** gibi avantajlar sağlayarak kritik altyapılar için uygun bir öğrenme paradigması sunmaktadır.

Ancak FL'de kullanılan **Güvenli Birleştirme (Secure Aggregation)** protokollerinin uygulaması sırasında, özellikle uç cihazların kısıtlı donanım özellikleri nedeniyle **yüksek enerji tüketimi**, **artmış gecikme süresi** ve **hesaplama yükü** gibi sorunlar ortaya çıkmaktadır. Bu bağlamda projede, bu üç temel amaç ayrı ayrı modellenerek bir çok amaçlı optimizasyon problemi oluşturulacak, ve bu fonksiyonlar arasında **Pareto optimal çözümler** geliştirmek hedeflenecektir.

Pareto optimalite, bir çözümün, herhangi bir amaç fonksiyonunu iyileştirirken diğerlerini kötüleştirmeden geliştirilemediği durumları tanımlar. Bu proje kapsamında, **enerji verimliliği**, **iletişim gecikmesi** ve **gizlilik düzeyi** arasında en iyi dengeyi sağlayan **Pareto ön sınırı (Pareto front)** üzerinde çözümler üretilecek; bu sayede her altyapı koşuluna uygun **dinamik şifreleme protokolleri** önerilecektir.

Bu amaçla, **Balina Optimizasyon Algoritması (WOA)** ve **Genetik Algoritma (GA)** gibi **meta-sezgisel algoritmalar** kullanılacak ve **çok amaçlı şifreleme optimizasyonu problemi** çözülecektir. Elde edilen sonuçlar, hem **sanal test ortamlarında** (ör. ICSSIM) hem de **gerçekçi veri setlerinde** (ör. Edge-IIoT) test edilerek performans analizine tabi tutulacaktır.

Proje çıktısı olarak, FL süreçlerinde görev yapan uç cihazlar için **enerjiye duyarlı**, **gizliliği yüksek** ve **gecikmesi düşük şifreleme çözümleri** geliştirilecek; bu sayede **kritik altyapılarda uçtan uca güvenli yapay zekâ uygulamaları** mümkün kılınacaktır. Proje, **ulusal siber güvenlik stratejilerine katkı** sağlayacak ve **kritik altyapılar için FL güvenlik çözümlerinde öncü bir yaklaşım** sunacaktır.

Araştırmacılar: Proje; yürütücü olarak Doç. Dr. Oğuzhan Ceylan'ın liderliği ve Prof. Dr. Hasan Dağ'ın danışmanlığında, iki doktora öğrencisi, bir yüksek lisans öğrencisi ve iki lisans öğrencisinden oluşan toplam yedi kişilik bir ekip (iki akademisyen ve beş bursiyer araştırmacı) tarafından yürütülecektir. Lisans ve lisansüstü araştırmacılar, Yönetim Bilişim Sistemleri, Elektrik-Elektronik Mühendisliği veya Bilgisayar Mühendisliği bölümlerinde aktif öğrencilikleri devam eden kişilerden seçilecektir. Proje süresince 4 iş paketi üzerinden 36 ay boyunca çalışmalar yürütülmesi planlanmaktadır.

Anahtar Kelimeler: Federe Öğrenme (FL), Güvenli Bir Araya Getirme (Secure Aggregation), Endüstriyel Kontrol Sistemleri (EKS), Maskeleme (Masking), Homomorfik Şifreleme (HE), MPC, Çok Amaçlı Optimizasyon, Balina Optimizasyon Algoritması, Genetik Algoritma, Siber Güvenlik ve Enerji Verimliliği

Title : Multi-objective Encryption Optimization within a Federated Learning Framework for Critical Infrastructures

Summary

Critical infrastructures—including **energy systems**, **transportation**, **communication**, and **healthcare**—are essential to both **national security** and the **continuity of societal functions**. The **Industrial Control Systems (ICS)** and **Internet of Things (IoT)** devices used in these systems are often **resource-constrained**, with **limited processing capabilities**, **energy**, and **bandwidth**. This makes **centralized AI models** inefficient or infeasible. **Federated Learning (FL)** offers a viable alternative by supporting **on-device training** and ensuring **data privacy** with **reduced communication latency**.

However, in FL, the use of **Secure Aggregation protocols** introduces significant overhead, especially when implemented on **low-power edge devices**. These protocols, relying on **masking**, **homomorphic encryption (HE)**, or **multi-party computation (MPC)**, can cause **high latency**, **excessive energy usage**, and **computational load**. Addressing this challenge requires a **multi-objective optimization** approach that balances these conflicting requirements.

This project aims to solve the multi-objective optimization problem based on three criterions to identify **Pareto optimal solutions**—those where **none of the key objectives (energy, latency, privacy) can be improved without compromising another**. The **Pareto front** will be used to provide **a range of optimized trade-off configurations**, tailored to different infrastructure types and device capabilities.

To this end, **metaheuristic algorithms** such as the **Whale Optimization Algorithm (WOA)** and the **Genetic Algorithm (GA)** will be employed to solve the **multi-objective secure aggregation optimization problem**. These methods will be tested and validated on both **virtual testbeds** (e.g., ICSSIM) and **realistic datasets** (e.g., Edge-IIoT), ensuring robust and comparative evaluation.

As a result, the project will develop **energy-aware**, **privacy-respecting**, and **low-latency secure aggregation protocols**, enabling the safe integration of **AI-based cyber threat detection systems** into **real-world critical infrastructure environments**. The outcomes will significantly contribute to **national cybersecurity frameworks** and pioneer a new direction in **secure federated learning architectures**.

The project will be carried out by a team of seven members in total—two academics and five scholarship-supported researchers—under the leadership of Assoc. Prof. Dr. Oğuzhan Ceylan (Principal Investigator) and with the guidance of Prof. Dr. Hasan Dağ. The team includes two doctoral students, one master's student, and two undergraduate students actively enrolled in Management Information Systems, Electrical-Electronics Engineering, or Computer Engineering programs. The research will be organized into four work packages and is planned to span 36 months.

Keywords: Federated Learning (FL), Secure Aggregation, Industrial Control Systems (ICS), Masking, Homomorphic Encryption (HE), MPC, Multi-Objective Optimization, Whale Optimization Algorithm, Genetic Algorithm, Cybersecurity, Energy Efficiency

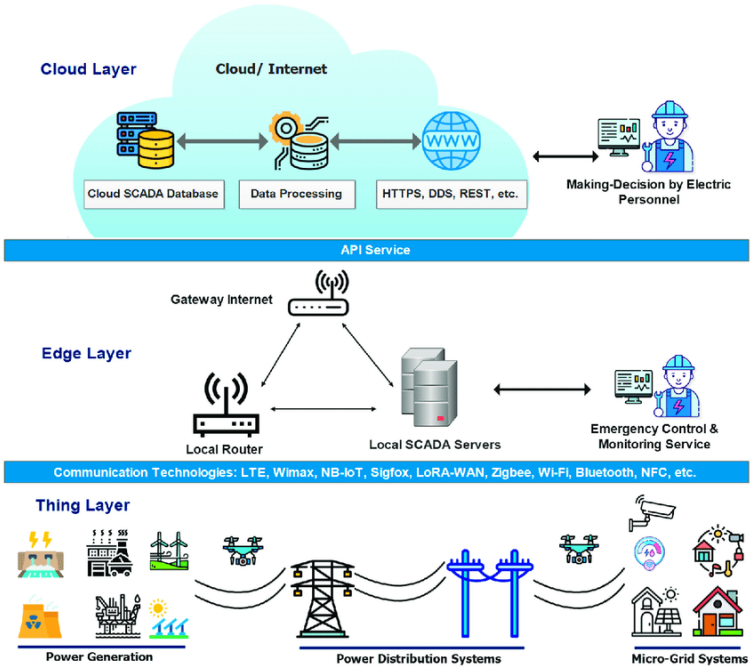
1. ÖZGÜN DEĞER

1.1. Konunun Önemi ve Projenin Özgün Değeri:

Kritik Altyapı Sistemleri (KAS), bilgi güvenliği ihlali durumunda can kaybına, ekonomik zararlara ve ulusal güvenlik açıklarına yol açabilecek bilişim ve endüstriyel kontrol sistemlerini kapsar [1]. Bu sistemler, hayati işlevler sundukları veya kritik bileşenler arasında bağlantı kurdukları için "kritik" olarak nitelendirilir [2]. **Federe öğrenme (FL) yaklaşımı**, verinin kaynak noktasında işlenebilme imkânı sayesinde merkezi sunuculara büyük veri aktarımının yarattığı gecikme, bant genişliği ve gizlilik risklerini azaltmada önemli bir rol oynar [1,2].

Özellikle **Merkezi Kontrol ve Veri Toplama (Supervisory Control And Data Acquisition – SCADA) sistemleri**, endüstriyel tesislerin ve kritik altyapıların merkezi kontrol ve izleme sistemleri olarak öne çıkmaktadır. Bu sistemler, üretim süreçlerinin, enerji dağıtımının, su ve atık yönetiminin yanı sıra ulaşım gibi hayati sektörlerin operasyonlarını denetler. Son yıllarda, SCADA sistemlerinin Şekil 1'de gösterilen üç katmanlı yapısının ilk (en alt) katmanındaki **IoT cihazlarının** yaygınlaşması, SCADA sistemlerine entegre edilen sensör, cihaz ve kontrol ünitesi sayısını artırmıştır. Bu entegrasyon, **akıllı izleme ve gerçek zamanlı veri toplama** gibi avantajlar sağlasa da, aynı zamanda siber saldırılara karşı yeni zafiyetler de getirmektedir.

Bu bağlamda, SCADA sistemlerinde IoT yapısı, hem **veri toplama** hem de **uzaktan izleme/denetim** açısından kritik bir öneme sahiptir. Ancak, IoT cihazlarının sınırlı işlem gücü, bellek ve enerji kapasiteleri, merkezi veri aktarımının risklerini ve performans darboğazlarını beraberinde getirmektedir. Bu durum, FL yaklaşımını daha da cazip hale getirirken, verinin yerinde işlenmesiyle siber saldırı yüzeyinin küçültülmesine olanak tanımaktadır.

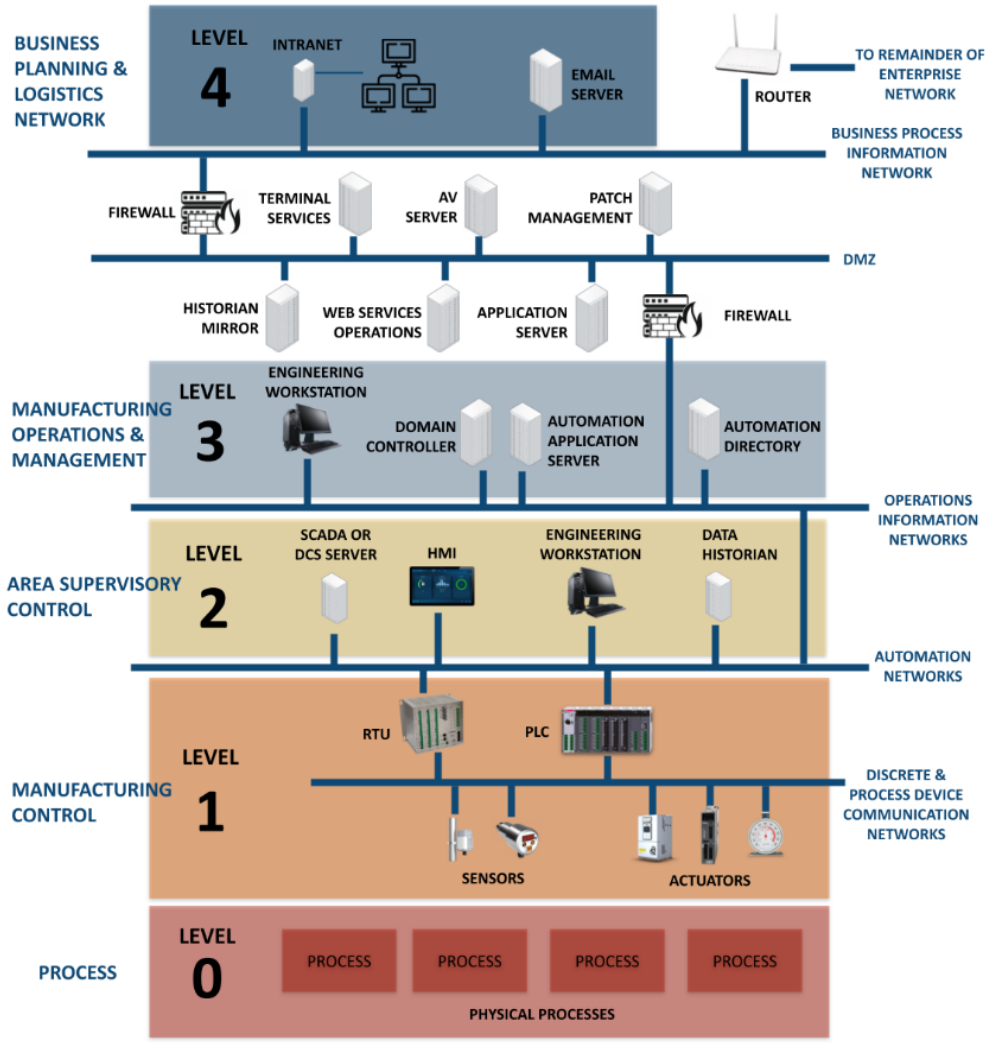


Şekil 1 - *Üç katmanlı SCADA yapısının bir örneği [12]*

Daha önce yürüttüğümüz ve tamamlanan bir TÜBİTAK 1001 projesinde (kod: 120E487), **FL ve metin analizi (BERT tabanlı)** üzerine çalışmalar gerçekleştirilmiştir. Bu projede, özellikle sistem günlüklerinden (log) yola çıkarak dağıtık ortamda saldırı/anomali tespiti yapılmış; ancak güvenli bir araya getirme protokollerinin detaylı optimizasyonu (ör. kriptografik parametre boyutları, gecikme-enerji dengesi) ve farklı protokol çeşitlerinin (maskeleme + MPC + HE) birlikte değerlendirilmesi kısıtlı kalmıştır. **Bu yeni çalışma**, önceki deneyimlerimizi geliştirerek, kriptografik yöntemlerin çok amaçlı optimizasyonla bütünleştirilmesini, daha yüksek saldırı dayanıklılığı, düşük gecikme ve daha verimli (daha düşük enerji) bir güvenli araya getirme protokolü oluşturmayı hedeflemektedir.

BT-OT Yakınsaması, bilgi teknolojileri (BT) ile operasyonel teknolojilerin (OT) entegrasyonunu ifade eder. BT veri merkezli çalışırken, OT fiziksel süreçleri yönetir; bu entegrasyon daha verimli fakat aynı zamanda daha savunmasız sistemler yaratmaktadır [3,4]. Endüstri 4.0 ve IoT ile sistemler giderek daha dağıtık ve bağlantılı hale gelmiş, bu durum siber saldırı yüzeyini genişleterek kritik altyapıların korunmasını daha da zorlaştırmıştır [5]. **Özellikle KAS'lerde**, Purdue Katmanlı Güvenlik Mimarisine (bknz: Şekil 2) göre farklı güvenlik protokollerinin uygulanması gerekliliği,

bütüncül bir yaklaşımın önemini ortaya koymaktadır [6,7].



Şekil 2 - *Purdue Modeli [13]*

Bu kapsamda, Stuxnet saldırısı (2010, İran'daki nükleer santral, Siemens kontrol sistemleri) siber savaş çağının başlangıcını simgelemektedir [8]. Sibirya boru hattı (1982), Chevron rafinerisi (1992), Worcester havalimanı (2007), Maroochy su-atık sistemi (2000) ve CSX tren hattı (2003) gibi örnekler, KAS'lerin zafiyetlerinin ne tür sonuçlar doğurabileceğini açıkça göstermektedir [9–11]. Bu olaylar, **geleneksel güvenlik önlemlerinin yetersizliğini** ve BT ile OT kayıtlarını işleyebilecek, doğal dil işleme ve federe makine öğrenimiyle desteklenmiş bütüncül savunma sistemlerinin gerekliliğini ortaya koymaktadır.

Endüstriyel Kontrol Sistemleri (EKS) ve IoT cihazları, bu altyapıların ayrılmaz parçası haline gelmiştir. Ancak bu cihazların ürettiği veriler çok hassas olup, işletim süreçlerini doğrudan etkilemektedir. **FL modeli**, katılımcı cihazların verilerini paylaşmadan yalnızca model güncellemelerini (parametre veya türev) iletmesi esasına dayanarak, verinin kaynaktan çıkartılmadan yerinde eğitilmesini sağlar [14,15]. Bu güncellemelerin gizliliğinin korunması zorunludur; aksi takdirde kötü niyetli saldırganlar parametre değerlerinden orijinal veri hakkında çıkarım yapabilir [15,21,29]. Bu noktada "Güvenli Bir Araya Getirme (Secure Aggregation)" protokolleri devreye girer. Literatürde maskeleme [14,15], homomorfik şifreleme (HE) [27,28] ve çoklu taraflı hesaplama (MPC) [18,29] gibi çeşitli yaklaşımlar bulunmasına rağmen, KAS'lerin yüksek hesaplama gereksinimleri ve IoT cihazlarının sınırlı donanımı nedeniyle pratikte istenen performansa erişmek zorlaşmaktadır.

Bu yaklaşımların avantajları ve dezavantajları aşağıdaki şekilde ele alınabilir:

1. **Maskeleme (Masking) Tabanlı Yöntemler:**
   Katılımcılar güncellemelerine rastgele gürültü (ya da maske) ekleyerek sunucuya iletir; toplu maske, yeterli

sayıda katılımcıdan sonra ortadan kaldırılarak toplam model güncellemesi elde edilir [14,15]. Bu yöntemin en büyük avantajı düşük hesaplama ve iletişim maliyetidir, fakat bir ya da birkaç katılımcının güncellemelerinin açığa çıkması durumunda maske tahmini riski bulunmaktadır [26].

2. **Homomorfik Şifreleme (HE) Tabanlı Yöntemler:**
   HE, şifrelenmiş veriler üzerinde toplama (ve bazen çarpma) işlemlerini, veriyi açığa çıkarmadan gerçekleştirmeye olanak tanır [27,28,31]. FHE (tam harmonik şifreleme), en geniş işlevselliğe sahip olmakla birlikte yüksek hesaplama maliyetleri ve bant genişliği tüketimi ile sınırlıdır. Kısmi HE uygulamaları, IoT gibi sınırlı kaynak ortamlarında yine de dikkatli optimizasyon gerektirmektedir [27].

3. **Çoklu Taraflı Hesaplama (MPC):**
   Veriler, birden fazla tarafa bölünerek (secret sharing) veya çeşitli şifreli paylar olarak saklanır. Sunucu ya da aracı taraflar, orijinal veriyi açığa çıkarmadan toplama işlemini yürütür [18,29]. Ancak, uç cihazlarda bağlantı kesintileri ve dropout durumları gibi sorunlar, MPC'nin IoT ağlarında uygulanmasını zorlaştırmaktadır [15].

Her yaklaşım, **gizlilik**, **hesaplama süresi**, **enerji tüketimi** ve **iletişim maliyeti** gibi farklı boyutlarda avantajlar ve dezavantajlar sunmaktadır [14,15,27]. Bu durum, düşük gecikme için maskeleme tercih edilirken; yüksek gizlilik için tam HE veya MPC'nin öne çıkabileceğini göstermektedir. Ancak, çok amaçlı durumlarda hangi protokolün hangi parametrelerle uygulanacağı literatürde henüz net bir çözüme kavuşmamıştır [22,29].

Optimizasyon yaklaşımları, FL protokollerinin karmaşık parametre uzayında en iyi çözümleri bulmak için kullanılmaktadır [16,17]. Örneğin; maskeleme düzeyi, HE'de anahtar boyutları, MPC'de taraf sayısı ve yedek mekanizmaların konfigürasyonu gibi değişkenler, meta-sezgisel algoritmalar (Genetik Algoritma (GA), Balina Optimizasyon Algoritması (WOA)) kullanılarak incelenebilmektedir [20,21]. Ancak, çoğu çalışma tek bir kriptografik yönteme odaklanmakta veya yalnızca tek bir performans metriğini optimize etmektedir [15,27]. **Literatürdeki boşluk**, maskeleme, HE ve MPC yaklaşımlarını aynı çerçevede, çok amaçlı maliyet fonksiyonları (enerji, gecikme, gizlilik) ile sistematik olarak değerlendiren yaklaşımların sınırlı olmasında yatmaktadır.

Bu boşluk, aşağıdaki şekilde özetlenebilir:

- **Protokol Çeşitliliği ve Optimizasyon Eksikliği:** Farklı protokollerin dinamik ağırlıklarla optimize edilmesi konusundaki çalışmaların azlığı [15,18,27].
- **Gerçekçi Veri ve Test Platformları:** Edge-IIoT [10] ve ICSSIM [24,25] gibi ortamların kısıtlı parametrelerle yapılan pilot testlerle sınırlandırılmış olması [14,15].
- **Aktif Saldırı ve Dropout Senaryoları:** Katılımcı cihazların ağdan kopması veya aktif saldırı durumlarının yeterince araştırılmaması [26,29].
- **Çok Amaçlı (Multi-objective) Optimizasyon:** Enerji, gizlilik ve gecikmenin beraberce değerlendirildiği fonksiyon modellerinin eksikliği [15,27].

Bu proje, **maskeleme, homomorfik şifreleme ve MPC protokollerini meta-sezgisel çok amaçlı optimizasyon** (Balina Optimizasyon Algoritması, Genetik Algoritma) bakış açısıyla aynı çatı altında birleştirmeyi amaçlamaktadır [16,17,20]. Deb'in çok amaçlı evrimsel optimizasyona dair öncü çalışmaları ([32]) ışığında, enerji, gecikme ve gizlilik gibi çatışan hedeflerin Pareto-optimal dengesinin belirlenmesi hedeflenmektedir. Böylece, hem **teorik** (yeni bir optimizasyon modeli ve protokol tasarımı) hem de **uygulamalı** (Edge-IIoT veri seti [23], ICSSIM sanal test yatağı [24,25] ve oluşturulacak benzetilmiş fiziksel test yatağı ile deneysel doğrulama) anlamda özgün katkılar sunulacaktır.

Kritik altyapılar (enerji şebekeleri, su dağıtımı, ulaşım vb.) açısından, FL'in sağladığı "veriyi yerinde işleme" avantajı kadar, sistemin **güvenlik** ve **hız** boyutunun da göz önünde bulundurulması gerekmektedir [24,25]. Bir siber saldırı senaryosunda, saldırganın model güncellemeleri üzerinden sistemin durumunu veya açıklarını tahmin edebilmesi büyük risk oluşturmaktadır [15,21]. Öte yandan, SCADA/PLC (Programlanabilir Mantıksal Denetleyici / Programmable Logic Controller) gibi ortamlarda komut ve sensör verilerinin gerçek zamanlı yönetimi gerekliliği, yüksek gecikme getiren protokolleri pratik açıdan işlevsiz kılmaktadır [27,31]. Bu nedenle, **gizlilik ile performans arasında uygun bir dengenin kurulması**, çözümü zor bir problem olarak literatürde öne çıkmaktadır [28,30].

Ayrıca, geleneksel şifreleme yöntemlerinin kuantum bilgisayarların gelişimiyle kırılabilir hale gelme riski, **post-kuantum saldırı senaryoları açısından** ek bir tehdit oluşturmaktadır [22,29]. Bu bağlamda, HE ve MPC tabanlı yöntemlerin güvenliği artırmak için daha büyük anahtar boyutları ve daha güçlü şifreleme seviyeleri gerektirmesi, gecikme ve enerji tüketimi sorunlarını derinleştirebilmektedir.

Uygulanabilirlik açısından, Edge-IIoT veri seti (IoT/IIoT saldırı çeşitliliği), ICSSIM ve oluşturulacak benzetilmiş fiziksel test ortamlarında yapılacak deneyler, çalışmanın **gerçek dünyayla bağlantısını güçlendirecek**; örneğin elektrik

şebekesi, su dağıtımı ve ulaştırma gibi altyapılarda FL tabanlı siber saldırı tespiti veya kestirim modellerinin geliştirilmesi, geleceğin akıllı şehir ve endüstri 4.0 uygulamalarının omurgasını oluşturacaktır [15,27].

Son olarak, projede hedeflenen **%15 enerji tasarrufu** ve **%30 gecikme azaltması** ölçütleriyle, uç cihazların ömrünün uzatılması ve sistemin gerçek zamanlı kontrol kabiliyetinin korunması sağlanacaktır [15,31]. Böylece, projemiz hem ulusal hem de uluslararası arenada kritik altyapı güvenliği ve federe öğrenme konularına önemli katkılar sunmayı amaçlamaktadır.

Bu çalışma, **güvenli, enerji verimli ve düşük gecikmeli bir federe öğrenme düzeni oluşturmak üzere** maskeleme, homomorfik şifreleme ve MPC protokollerini meta-sezgisel çok amaçlı optimizasyon modelleriyle **entegre eder**. Böylece, "Hangi ortamda hangi protokol nasıl konfigüre edilmeli?" sorusuna sistematik ve dinamik bir yanıt getirerek, literatürdeki önemli boşluğu doldurmayı amaçlamaktayız.

1.2. Araştırma Sorusu ve/veya Hipotezi:

Araştırma Sorusu:
"Kritik altyapılarda (EKS/IoT) yüksek güvenlik ve performans gerektiren federe öğrenme senaryolarında, hangi güvenli toplama protokolleri nasıl optimize edilerek hem gizlilik hem de enerji/hesaplama verimliliği sağlanabilir?"

Hipotez:

"Balina Optimizasyon Algoritması, Genetik Algoritmalar gibi çok amaçlı optimizasyon yöntemleri ile homomorfik şifreleme/maskeleme tabanlı güvenli toplama protokolleri iyileştirilerek, en az %15 enerji tasarrufu ve %30 gecikme azalması elde edilebilir; kritik altyapılarda veri bütünlüğü ve gizlilik riski en aza indirgenir."

Yukarıdaki araştırma sorusu, **kritik altyapıların** operasyonel ihtiyaçları doğrultusunda iki ana bileşenden oluşur: **(i) gizlilik**, **(ii) performans**. EKS/IoT sistemlerinde verilerin taşınmasıyla gelen siber saldırı ve gizlilik risklerini asgariye indirme gereksinimi, **güvenli toplama protokollerinde** (masking, HE, MPC) güncel teknolojik yaklaşımların derinlemesine incelenmesini zorunlu kılmaktadır [15,18]. Ancak farklı protokollerin uygulanması, genellikle **hesaplama gücü**, **enerji tüketimi**, **iletişim gecikmesi** gibi kritik faktörleri beraberinde getirir. Bu nedenle projemizde, "bu protokolleri nasıl optimize edebiliriz?" sorusunu sormakta ve cevap aramaktayız.

Hipotez kısmında belirlenen, **en az %15 enerji tasarrufu ve %30 gecikme azalması** hedefi, literatürde rapor edilen tipik maskeleme/HE/MPC tabanlı FL deneyleriyle kıyaslandığında önemli bir iyileşmeyi ifade etmektedir [15,27,28]. Özellikle mobil veya gömülü IoT cihazlarda homomorfik şifrelemenin hesaplama yükünü hafifletmek ve paket sayısını azaltmak için geliştirilecek mekanizmaların mevcut denemelerden daha verimli olacağı değerlendirilmektedir. Ayrıca projede kullanılacak WOA ve GA gibi meta-sezgisel yöntemlerin literatürde %10–20'a varan iyileştirmeler sağladığı rapor edilmiştir [16,17,20]. Buradan hareketle, kritik altyapılar özelinde daha yüksek oranda iyileşmenin mümkün olabileceği varsayılmaktadır.

Ek olarak, proje, sadece **teorik** düzeyde bir güvenlik artışı iddia etmekle kalmayıp, **pratikte** Edge-IIoT veri seti [23] üzerinde siber saldırı tespiti senaryosuyla, ICSSIM [24,25] ve fiziksel benzetilmiş test yatağı üzerinde endüstriyel kontrol senaryolarıyla etkinliğini ölçecektir. Bu uygulama boyutu, hipotezdeki öngörülerin test edilebilirliğini sağlamaktadır.

1.3. Amaç ve Hedefler:

Amaç:
Kritik altyapılarda kullanılan EKS ve IoT cihazlarında federe öğrenmeyi gizlilik ihlallerinden koruyarak gerçek zamanlı ve enerji tasarruflu hâle getirecek yeni protokolleri ve optimizasyon modellerini geliştirmek.

Hedefler:

1. Varolan güvenli bir araya getirme (maskeleme, homomorfik şifreleme, MPC) yöntemlerinin EKS/IoT bağlamında analizini yapmak.
2. Doç. Dr. Oğuzhan Ceylan'ın önceden elektrik güç sistemlerindeki çok amaçlı optimizasyon problemlerini çözdüğü çalışmalarından yararlanarak çok amaçlı bir fonksiyon tanımlamak ve algoritmaları (WOA, GA) entegre etmek.
3. Edge-IIoT veri seti, ICSSIM sanal test yatağı ve geliştirilen fiziksel benzetilmiş test yatağında güvenli

FL prototipini doğrulamak.

4. Proje sonunda en az 2 SCI makale, 2 konferans bildirisi ve sektörel iş birliği raporları üretmek.

Bu amaç ve hedefler, projenin çıktılarını **ölçülebilir** ve **somut** hâle getirmektedir. Örneğin:

1. **Gereksinim analizi**: Mevcut protokollerin hem akademik hem de endüstriyel raporları incelenerek, EKS/IoT ortamlarında hangi parametrelerin (Maskeleme parametreleri, Homomorfik şifreleme anahtar boyutu, MPC taraf sayısı, İletişim tur sayısı, Uç cihaz sayısı, Veri boyutu) kritik olduğu belirlenecektir [14,15,22]. Bu analiz, hangi protokolün hangi koşullarda avantaj veya dezavantaja sahip olduğunu nicel verilere dayalı olarak ortaya koyacaktır.

2. **Çok amaçlı optimizasyon problemi**:

Gecikme süresi: $T(x)=T_{\text{comm}}+T_{(\text{comp})}(minimize)$ Enerji Tüketimi: $E(x)=\sum(P_i\times t_i)+E_{\text{comm}})(minimize)$ Gizlilik Düzeyi: $P(x)=\log_2(M)+\alpha\cdot k+\beta\cdot t)(maksimize)$	(1)

Bu üç hedef amaç, **Balina Optimizasyon Algoritması (WOA)** ve/veya **Genetik Algoritma (GA)** ile **Pareto-öncelikli** bir çerçevede optimize edilecektir [16,17,20,32]. Tek bir ağırlıklı fonksiyon yerine, **dominasyon** (baskın gelme) ilkesi kullanılarak **farklı denge noktaları** (trade-off) keşfedilecektir.

3. **Prototip doğrulaması**: Projede, **Python/C++** tabanlı modüllerle gerçekleştirilecek prototip hem **Edge-IIoT veri seti** ([23,27]) üzerinde siber saldırı tespitine, hem de **ICSSIM** ([24,25]) üzerinde sanal olarak ve oluşturulacak fiziksel benzetilmiş test yatağında fiziksel olarak SCADA benzeri endüstriyel süreç kontrollerine uygulanacaktır. Başarı göstergeleri arasında "toplam gecikme süresi", "enerji tüketimi" (ör. Raspberry Pi benzeri cihazlarda ölçülen) ve "olası saldırı senaryolarına karşı gizlilik dayanıklılığı" yer alacaktır.

4. **Yayın ve iş birliği**: Projenin akademik katkısı, en az 2 SCI makale ve 2 konferans bildirisiyle somutlaşacaktır. Ek olarak, sektörle yapılacak atölye veya demo çalışmaları, **gerçek saha** uygulamalarına da kapı aralayacak; geliştirilen prototip, farklı kurumların test ortamlarında (örneğin elektrik dağıtım şirketleri) denenebilecektir.

Yukarıda verilen **açık, ölçülebilir ve ulaşılabilir** hedeflerin, projenin 36 aylık çalışma takvimi içerisinde gerçekleştirilmesi planlanmaktadır. Ayrıca projenin hedefleri, **kritik altyapıların güvenli dijital dönüşümü** ve **ulusal siber güvenlik** stratejileriyle de uyum göstermektedir [15,27].

2.YÖNTEM

2.1. Araştırma Tasarımı ve Aşamalar

Proje, **dört temel aşamadan** oluşan bir araştırma tasarımına sahiptir. Bu aşamalar, **girişte belirtilen** amaç ve hedefler doğrultusunda hem kuramsal hem de uygulamalı yöntemlerden oluşmaktadır. Proje süresince **bağımlı değişkenler** olarak:

1. **Gizlilik Düzeyi** (örneğin saldırganın model güncellemelerinden veri sızdırabilme olasılığı ya da matematiksel bir gizlilik metriği),
2. **Gecikme Süresi** (iletişim ve işlem gecikmesi),
3. **Enerji Tüketimi** (uç cihazlar için toplam güç sarfiyatı)

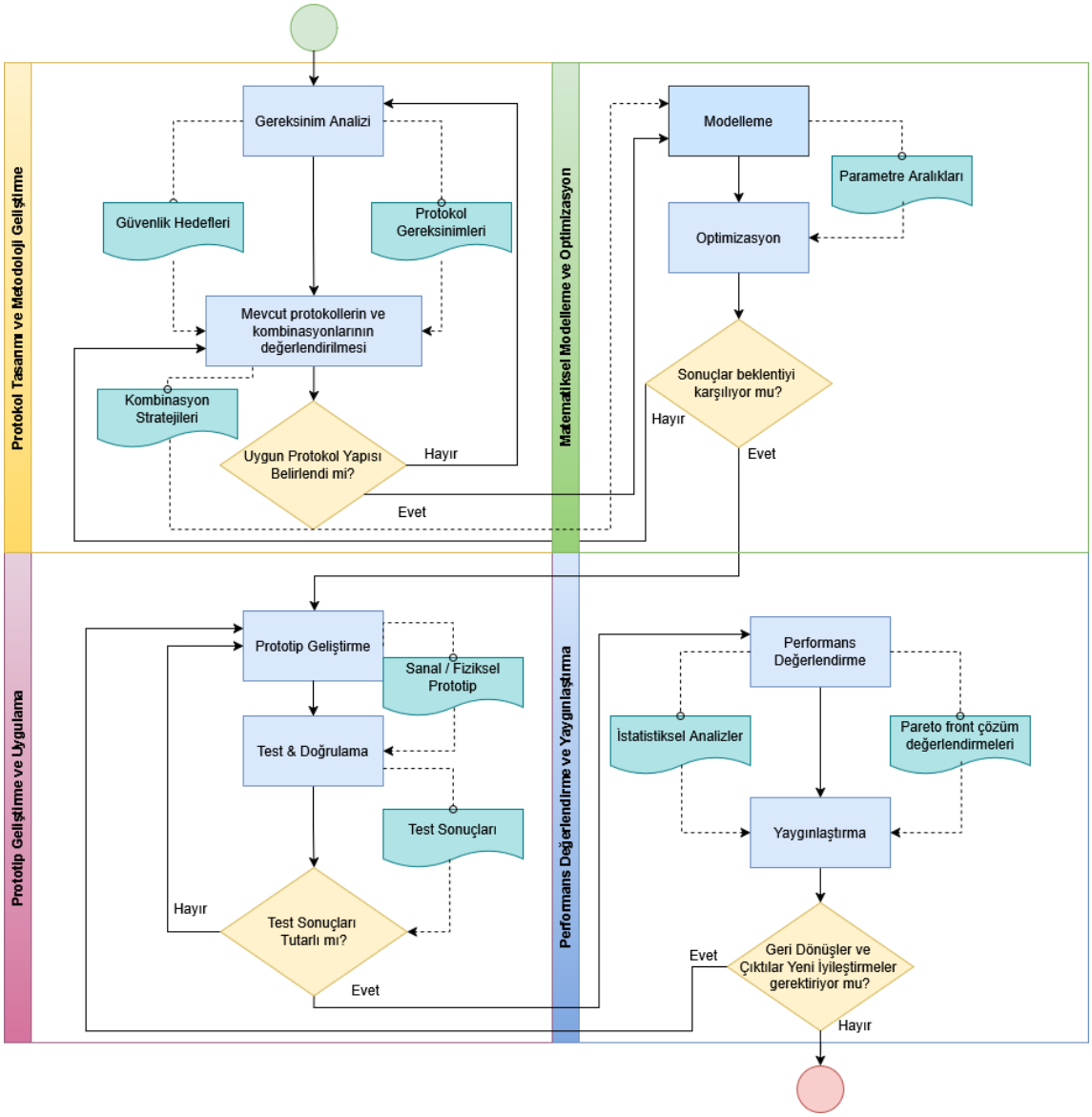
belirlenmiştir. Buna karşın bağımsız değişkenler, yani projede kontrol ettiğimiz veya değiştirdiğimiz değişkenler:

- Protokollerin kriptografik parametreleri,
  - Maskeleme parametreleri
  - Homomorfik şifreleme anahtar boyutu
  - MPC taraf sayısı
- İletişim tur sayısı,
- Uç cihaz sayısı,

- Veri boyutu,

olarak belirlenmiştir [15,27,28].

Aşağıda **Şekil 3'de**, yöntemin genel akışını özetlenmektedir .



***Şekil 3** - Yöntem Akış Şeması*

Bu şemada, her aşamanın çıktı(lar)ı bir sonraki aşamaya girdi sağlar. Örneğin, **Protokol Tasarımı** sonucunda belirlenecek parametre aralıkları ve güvenlik senaryoları ile teknik tasarım, **Matematiksel Modelleme** fazında kullanılacak yöntem ve değerlere rehberlik edecektir.

2.2. Protokol Tasarımı ve Metodoloji Geliştirme

Bu aşamada, projenin dayandığı **güvenli bir araya getirme** (Secure Aggregation) protokollerinin mevcut durumu incelenmektedir. Özellikle:

- **Maskeleme**: Mevcut çalışmaların çoğu, verileri rastgele gürültü veya maskeleme anahtarları ile gizlemeyi önerir. Ancak pasif saldırılara karşı belli riskler, aktif saldırı durumunda ise çoklu maske paylaşım stratejilerinde karmaşıklık söz konusudur [14,15,28].
- **Homomorfik Şifreleme (HE)**: Tam (fully) homomorfik şifreleme gizlilik açısından iyi çalışsa da büyük hesaplama maliyeti vardır. Kısmi (partial) veya tam homomorfik şifrelemenin EKS/IoT uygulamalarında bant

genişliği ve işlem süresi kısıtlarını aşmak zordur [27,28,31].

- **MPC (Çoklu Taraflı Hesaplama)**: Eş zamanlı (synchronous) veya kısmen eş zamansız (asynchronous) modellerde uygulanabilir. Ancak birden çok tarafın sürekli çevrim içi olması ve güvenilir kanallara ihtiyaç duyması, IoT ağlarında zorluklar getirmektedir [18,29].

Gereksinim analizi kapsamında, EKS/IoT ortamlarda:

- **Gerçek zamanlılık**: SCADA sistemleri ve IoT cihazlarındaki karar mekanizmalarının düşük gecikme eşiği,
- **Hata toleransı (fault tolerance)**: Bazı uç cihazların ağdan düşmesi (dropout) veya iletişim hatalarının olması.
- **Düşük enerji tüketimi**: Büyük ölçekte binlerce IoT düğümünün bataryayla çalıştığı senaryolar,
- **Veri gizliliği ve güvenliği:** Kritik altyapılarda şifrelenmiş veri işleme ihtiyacı ve güvenlik risklerinin en aza indirilmesi,
- **Kaynak kısıtlarıyla uyumluluk:** Bellek, işlem gücü ve bant genişliği sınırlı olan uç cihazlar için optimize edilmiş çözümler geliştirilmesi,

özellikle homomorfik şifreleme (HE) ve güvenli çoklu taraf hesaplama (MPC) gibi veri güvenliği mekanizmalarının entegrasyonu sırasında dikkate alınmalıdır.

Edge-IIoT veri seti [23] ve **ICSSIM** [24,25] platformları burada temel gereksinimleri temsil eden örnekler olarak verilebilir. Edge-IIoT veri seti, IoT ve IIoT (Endüstriyel IoT) saldırı çeşitlerini ve normal trafik örneklerinden oluşur, dolayısıyla protokolün **siber saldırı tespiti** senaryosuna uygulanabilir. ICSSIM ise SCADA ve endüstriyel kontrol bileşenlerini mikro hizmet tabanlı bir şekilde simüle ederek, EKS ortamlarında protokol testine olanak tanır.

Bu aşamada belirlenecek **kritik parametreler** (Maskeleme parametreleri, Homomorfik şifreleme anahtar boyutu, MPC taraf sayısı, İletişim tur sayısı, Uç cihaz sayısı, Veri boyutu) ve **performans ölçütleri** (gizlilik seviyesi, gecikme, enerji) bir sonraki aşamalarda kullanılacaktır [15,22].

Protokol tasarımı aşamasında, maskeleme, HE ve/veya MPC yaklaşımlarının **bir arada** veya **ikili kombinasyon** hâlinde nasıl uygulanacağı tanımlanacaktır. Örneğin:

1. **Maskeleme + Homomorfik Şifreleme (HE)**: Gradyan'lar önce hafif düzeyde maske ile gizlenir, ardından kısmi homomorfik şifreleme uygulanır [27,28]. Bu şekilde tam HE yerine kısmi HE (ör. BFV, BGV) ile daha düşük işlem maliyeti hedeflenir.

2. **MPC + Maskeleme**: Model parametreleri farklı taraflar arasında paylaştırılır (secret sharing), aynı zamanda pasif saldırı riskine karşı ek gürültü eklenir [18,29].

3. **Yalnızca Homomorfik Şifreleme veya Yalnızca Maskeleme**: Bazı uç cihazlarda tam kriptografik işlem gücü yetersizse sadece maskeleme kullanılabilir. Bu durum, "heterojen protokol" senaryosu olarak tasarlanabilir.

Protokol Adımları ve Dropout Yönetimi

Protokol, pasif ve aktif saldırılara karşı nasıl çalışacağını tanımlarken, aynı zamanda uç cihazların (örn. IoT sensörler) **her hesaplama döngüsünde (turda) çevrim içi olmayabileceğini** de göz önünde bulundurmalıdır. **Federated Learning (FL)** veya **güvenli çoklu taraf hesaplama (MPC)** gibi senaryolarda, uç cihazlar çeşitli nedenlerle belirli turlarda ağa katılamayabilir veya veri paylaşamayabilir. Bu durum, model güncellemesi ve güvenlik açısından **dropout resilience** (katılımcı uç cihazların bağlantı kesintilere karşı dayanıklılığı) **mekanizmalarının** kritik hale gelmesine neden olur.

Örneğin, **dropout'a dayanıklı (dropout resilient) yaklaşımlar** ([26]), **maskeleme anahtarlarının paylaşımı gibi veri bütünlüğünü ve gizliliğini koruyan stratejileri içerir.** Eğer bir uç cihaz belirli bir turda çevrim dışı kalırsa, protokolün bu kaybı nasıl yöneteceği ve güvenliği nasıl sağlayacağı iyi tanımlanmalıdır. Bu tür mekanizmalar, eksik veri nedeniyle hesaplamanın sekteye uğramasını engelleyerek hem sistemin sürekliliğini sağlar hem de güvenlik açıklarının oluşmasını önler.

Bir örnek protokol akışının maddelerini içeren **Tablo 1** aşağıda verilmiştir:

Tablo 1 *- Protokol Akış Tablosu*

Adım	Açıklama	Referans
1. Anahtar/Gürültü	Uç cihazlar, maskeleme için rastgele gürültü değerlerini veya HE için anahtar	[2], [14],

Oluşturma	çiftlerini üretir.	[15]
2. Öğrenme Turu Başlatma	Cihazlar, lokal eğitim (ör. mini-batch gradient descent) sonrasında güncelleme parametrelerini hazırlamaya başlar.	[1], [6], [13]
3. Şifreleme / Maskeleme	Güncellemeler, seçilen protokole göre şifrelenir veya maskeleme uygulanır. (Kısmi homomorfik / tam HE)	[14], [18]
4. Toplama (Aggregation)	Sunucu veya MPC paydaşları, alınan şifreli / maskelenmiş parametreleri toplar. Gizlilik ihlali olmayacak şekilde partial decrypt veya maske çıkarma işlemi gerçekleştirilir.	[5], [16]
5. Model Güncellemesi	Toplam sonucu geri dağıtan sunucu/ortak noktalar, yeni global modeli duyurur. Dropout olan cihazlar bir sonraki turda kaldıkları yerden devam ettirilebilir.	[2], [13]
6. Kontrol ve Tekrar	Tur tamamlanır, protokol parametreleri (örn. maske yenileme sıklığı, homomorfik şifreleme anahtar geçerliliği) güncellenerek istenen tur sayısınca devam edilir.	[1], [2], [14]

Güvenlik Analizi: Pasif saldırgan, uç cihazın veya sunucunun gönderdiği veriyi dinleyebilir ancak manipüle etmez. Aktif saldırgansa manipülasyon veya sahte veri ekleme gibi ek tehditler sunar. Protokol tasarımında bu farklılıklar göz önüne alınarak, **ortak anahtar değişimi**, **rastgele maske sıfırlama** aralıkları ve **MPC taraflarının yedekli (redundant) yönetimi** planlanacaktır [15,29].

2.3. Matematiksel Modelleme ve Optimizasyon

Bu projede, **güvenli toplama (Secure Aggregation) protokolü** için tanımlanan maliyet kalemlerinin ve performans ölçütlerinin **çok amaçlı (multi-objective) bir optimizasyon** yaklaşımıyla ele alınması hedeflenmektedir. Literatürdeki bazı çalışmalarda [16,17,20] **tek bir ağırlıklı amaç fonksiyonu** kullanılsa da, **Deb (2001)** prensiplerine dayanarak [32] **Pareto-öncelikli çok amaçlı optimizasyon** yaklaşımı benimsenmiştir. Bu sayede, **enerji tüketimi (E)**, **gecikme süresi (T)**, ve **gizlilik (P)** gibi **üç farklı metriğin** aynı anda değerlendirilmesi ve **farklı denge noktalarının** (trade-off) keşfedilmesi sağlanacaktır.

2.3.1. Maliyet ve Performans Fonksiyonları

Aşağıda sırasıyla **gecikme (T)**, **enerji (E)**, ve **gizlilik (P)** metrikleri tanımlanmakta ve projedeki önemleri açıklanmaktadır. Her metrik, **ayrı bir amaç fonksiyonu** olarak ele alınır.

(a) Gecikme Süresi (T)

Toplam gecikme, **iletişim** (T_{comm}) ve **işlem** (T_{comp}) gecikmelerinin bileşimi olarak ifade edilebilir [15,27]:

$$T = T_{\text{comm}} + T_{\text{comp}} \tag{2}$$

- T_{comm}: Uç cihazlardan sunucuya (veya MPC taraflarına) veri gönderme/alma süresi.
- T_{comp}: Şifreleme, maskeleme ve toplama (aggregation) işlemleri sırasında oluşan işlem süresi.

Amaç: Gecikme T değerini **minimize etmek**, zira EKS/IoT gibi gerçek zamanlı karar gerektiren ortamlarda **düşük**

gecikme kritik önemdedir.

(b) Enerji Tüketimi (E)

IoT cihazlarında enerji tüketimi, işlemci (CPU/GPU) kullanımı ve kablosuz iletişim maliyetiyle modellenebilir [14,19]:

$$E = \sum_{i=1}^{N} \left(P_i \times t_i \right) + E_{\text{comm}} \tag{3}$$

- P_i: İlgili cihazın ortalama güç çekişi (Watt).
- t_i: İlgili işlem için harcanan süre (saniye).
- E_{comm}: Veri gönderimi/alımı için harcanan enerji.

Amaç: Enerji E değerini **minimize etmek**, zira özellikle **binlerce uç cihazın** pil (batarya) ile çalıştığı geniş ölçekli IoT senaryolarında **enerji tasarrufu** hayati önem taşır.

(c) Gizlilik Metriği (P)

Gizlilik metriği, pasif/aktif saldırılara karşı protokolün kırılma olasılığı veya saldırganın veri geri kazanma ihtimalinin **zorluğu** üzerinden tanımlanabilir [18,22,29]. Literatürde, bu metriği **sayısal** hale getiren farklı formüller bulunmaktadır. Örnek olarak [27,30]:

$$P = f(M, k, t) = \log_2(M) + \alpha \cdot k + \beta \cdot t \tag{4}$$

- M: Şifreleme/maskeleme uzayının büyüklüğü (olası anahtar veya maske kombinasyon sayısı).
- k: Kriptografik parametre (örn. anahtar boyutu, taraf sayısı).
- t: Zamanla ilgili güvenlik değişkeni (örn. anahtar yenileme periyodu).
- α, β: Her bir parametrenin gizliliğe katkı katsayıları.
- $\log_2(M)$: Anahtar uzayının bit cinsinden büyüklüğünü yansıtır; saldırganın çözmek zorunda olduğu kombinasyon sayısı.

Amaç: Gizlilik P değerini **maksimize etmek**.

2.3.1.1. Pareto-Temelli Çok Amaçlı Optimizasyon

Projede, **T** ve **E minimize**, **P** ise **maksimize** edilmesi gereken **üç hedef** şeklinde ele alınır. **Deb (2001)** yaklaşımına göre [32], **tek bir bileşik fonksiyon** (ör. F(x)=αE+βT−γP) kullanmak yerine, **Pareto optimizasyonu** uygulanır. Bu sayede:

- **Dominasyon İlkesi**: Bir çözüm **x**, başka bir çözüm **y** tarafından **tamamen domine edilmediği** sürece **Pareto optimal** olabilir.
- **Pareto front (Pareto Öncelikli)**: Sistemin bulduğu **domine olmayan** çözümler kümesi. Burada **farklı denge noktaları** (ör. düşük E–düşük T, orta P gibi) aynı anda bulunabilir.
- **Senaryoya Göre Seçim**: Kritik altyapı yöneticileri, Pareto front üzerindeki çözümlerden **o anki ihtiyaçlara** (pil durumu, saldırı riski vb.) göre seçim yapabilir.

Bu yaklaşım, **kısıtlı kaynak** (IoT) ve **yüksek güvenlik gereksinimi** (EKS) ortamlarının **dinamik** ve **çok boyutlu** doğasına daha iyi uyum sağlar.

Projede ele alınan üç ayrı hedefin—örneğin gecikme süresi (T), enerji tüketimi (E) ve gizlilik (P)—her birinin farklı yönlerde optimize edilmesi gerektiğinde (iki metrikte değerin minimize edilmesi, bir metrikte değerin maksimize edilmesi gibi), **Pareto optimizasyonu** en uygun yaklaşım olarak öne çıkmaktadır. Bu yöntemin temel fikri, tek bir toplu maliyet fonksiyonu tanımlamak yerine, birbirleriyle çelişkili hedefleri **aynı anda** göz önünde bulundurarak en "dengeli" çözümleri (**Pareto optimal çözümler**) bulmaktır [32].

1. **Dominasyon İlkesi**
   Herhangi bir çözümün x, hem gecikme hem de enerji gibi farklı hedeflerde başka bir çözümden y *daha kötü (veya eşit ve birinde daha kötü)* olmadığı sürece, o çözüm domine edilmemiş sayılır. Dolayısıyla x, sistemin farklı ihtiyaçlarını bir bütün olarak "daha az tatmin eden" herhangi bir çözümden baskın olurken, tam tersi bir çözümle karşılaşmazsa *Pareto optimal* kabul edilir.

2. **Pareto Front (Pareto Ön Cephesi)**
   Dominasyon analizi sonucunda elde edilen, hiçbir çözümün bir diğerini tam olarak alt edemediği (ya da "geçemediği") **domine olmayan çözümler kümesi**, *Pareto front* olarak adlandırılır. Pareto front'taki her çözüm, farklı bir **denge noktası** (trade-off) ortaya koyar:

   - **Enerjiyi daha da azaltmak isterseniz** gecikme ya da gizlilik maliyeti yükselir.
   - **Gecikmeyi biraz daha düşürmek isterseniz** enerji tüketiminin artmasını göze almanız gerekebilir.

3. **Senaryoya Göre Seçim**
   Kritik altyapı yöneticileri (veya karar vericiler), **Pareto front** üzerinde yer alan herhangi bir çözümü, o anki **ihtiyaca göre** seçebilirler. Örneğin:

   - **Saldırı riski yüksek bir dönemde** gizliliği en üst düzeye çıkaran çözüme doğru kayabilirler (ki bu durumda gecikme ve enerji tüketimi artabilir).
   - **Bataryası sınırlı IoT cihazlarının** bulunduğu bir senaryoda, enerji tüketimini minimumda tutan Pareto noktasını tercih edebilirler.

Bu esneklik, **kısıtlı kaynak (IoT) ve yüksek güvenlik gereksinimi (EKS) ortamlarının dinamik ve çok boyutlu doğasına** uyumlu olduğu için Pareto-temelli yaklaşım projede kritik bir rol oynamaktadır.

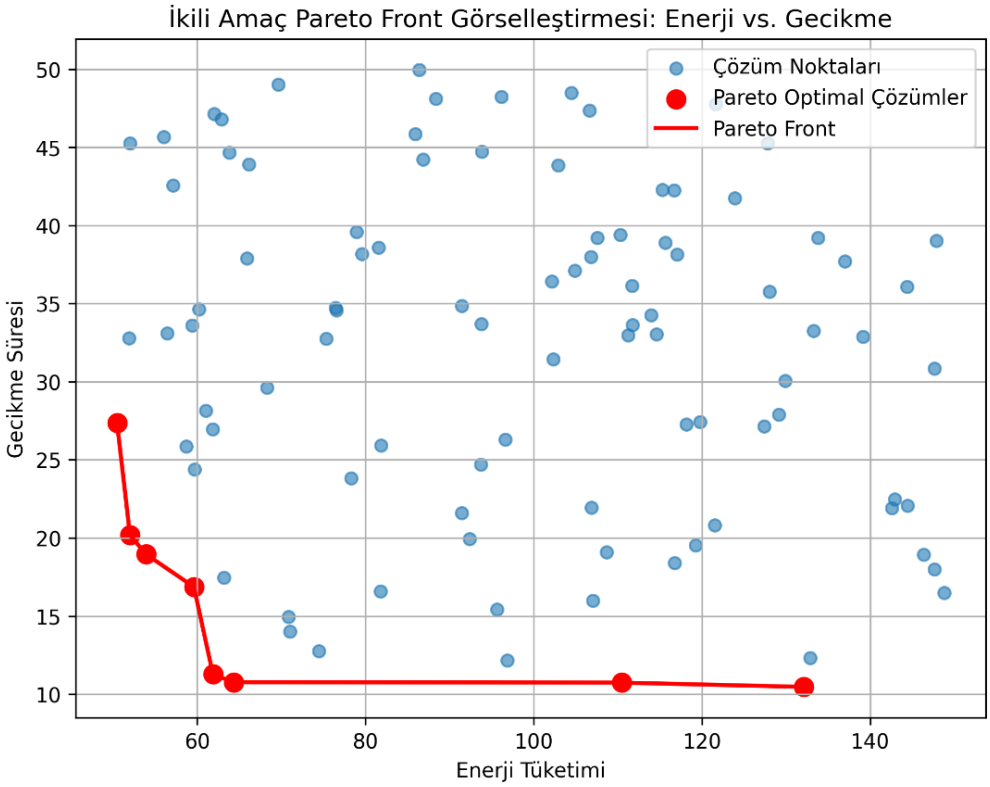
Pareto Front Örneği: Gecikme (T)- Enerji (E) İlişkisi

Aşağıdaki **Şekil 4**'de, gecikme ve enerji olmak üzere **iki amaçlı** bir optimizasyon problemi için Pareto çözüm örneği sunulmuştur. Mavi noktalar, rastgele veya deneysel olarak elde edilmiş potansiyel çözüm noktalarını temsil etmektedir. Dikey eksende gecikme süresi (ms, saniye), yatay eksende ise enerji tüketimi (Joule, Watt-saat) yer almaktadır.

- **Mavi Noktalar (Tüm Çözümler):** Farklı parametrelerle elde edilen çözüm veya senaryolar.

- **Kırmızı Noktalar (Pareto Optimal Çözümler):** Bu noktalardan *her biri*, en az bir başka çözümden hem enerji hem de gecikme bakımından daha kötü durumda olmadığı için *domine edilmemiş*tir.

- **Kırmızı Çizgi (Pareto Front):** Bu kırmızı noktaların birbirleriyle birleştirilmesiyle oluşan eğri, "en iyi denge noktaları"nı bir arada gösterir. Pareto front, projede T,E,P gibi çoklu hedefler birlikte ele alındığında 2B yerine 3B (hatta daha yüksek boyutlu) uzayda düşünülebilir; burada ise örnek amaçlarla iki boyutta T ve E gösterilmiştir.



Şekil 4 - *İkili Amaç Pareto Front Görselleştirmesi: Enerji vs. Gecikme*

Bu grafikten şu bilgiler çıkarılabilir:

- Sol alt köşede bulunan Pareto noktaları, hem düşük enerji hem de düşük gecikme hedefini **oldukça iyi** yakalayabilir; fakat **diğer metrikler** (ör. gizlilik, saldırı dayanıklılığı) bu noktada göz ardı edilebilir.
- Pareto front boyunca ilerledikçe, bir metrikte daha iyiye gitmek istendiğinde, diğer metrikteki kayıp (ör. daha yüksek enerji, daha uzun gecikme) **kaçınılmaz** olabilir.
- Gerçek verilerle çalışıldığında (örneğin projemizde Edge-IIoT veri seti, test yatağı ortamları), optimizasyon algoritmalarından (WOA, GA) elde edilen bu **Pareto ön cephe** üzerinden karar vericiler, **sistem gereksinimlerine** göre ideal noktayı seçebilir.

Böylece Pareto-temelli çok amaçlı optimizasyon, proje kapsamındaki **enerji, gecikme, gizlilik** gibi çelişkili hedefleri dengeleyerek, kritik altyapı ve IoT cihazlarının **gerçek zamanlı**, **kaynak verimli** ve **güvenli** bir şekilde çalışmasına önemli katkı sağlamaktadır.

2.3.2. Optimizasyon Yaklaşımları

Çok amaçlı optimizasyon problemini çözmek için proje kapsamında **Balina Optimizasyon Algoritması (WOA)** ve **Genetik Algoritma (GA)** gibi **meta-sezgisel** yöntemler [16,17,20,21] kullanılacaktır. Literatürde, her iki algoritmanın da **tek amaç** veya **çok amaç** fonksiyonlar üzerinde başarılı uygulamaları bulunmaktadır. Bu çalışmada, **Pareto tabanlı** sürümleri tercih edilerek, **dominasyon, non-dominated sorting, crowding distance** gibi kavramlar yardımıyla **Pareto front** elde edilecektir [32].

2.3.2.1. Balina Optimizasyon Algoritması (WOA)

Balina Optimizasyon Algoritması, **kambur balinaların "bubble-net" avlama davranışını** taklit eden bir yöntemdir [3], [4],[7]. Temel aşamalar şunlardır:

1. **Daire Çizerek Kuşatma (Encircling Prey)**:
   Balinalar, "av" olarak kabul edilen çözümlerin etrafında daire çizerek yaklaşır.
2. **Baloncuk Ağ (Bubble-Net) Stratejisi**:
   Logaritmik spiral hareketiyle, **dairesel** ve **radyal** bileşenlerin birleşimiyle konum güncellenir.
3. **Rastgele Avlama (Exploration)**:

Henüz iyi bir çözüm bulunamadığında veya yerel minimumdan kaçmak istendiğinde, farklı konumlara hareket sağlanır.

Pareto Tabanlı WOA:

- Tek bir "en iyi" çözüm aramak yerine, popülasyon içinde **baskın olmayan** çözümler bir öncü (elit) küme olarak saklanır.
- Her iterasyonda, balinalar bu **Pareto front** üzerindeki farklı çözümlere göre konumlarını güncelleyerek, **farklı amaçlar** (T, E, P) açısından iyi performans gösteren çözümleri keşfeder.

Proje bağlamında, bir **balina** (yani aday çözüm) şu parametreleri içerebilir:

$$x = [\text{MaskingLevel}, \text{HEKeySize}, \text{MPCParties}, \text{CommunicationRoundCount}, \ldots] \quad (5)$$

Her iterasyonda, **Pareto-öncelikli** yaklaşım sayesinde, enerji ve gecikmeyi düşürürken gizliliği de mümkün olduğunca **yükseltmeye** çalışılır [32].

2.3.2.2. Genetik Algoritma (GA)

Genetik Algoritma (GA), **doğadaki genetik evrim** sürecini (seçim, çaprazlama, mutasyon) modelleyen bir meta-sezgisel yöntemdir [16,21].

- **Seçim (Selection)**: Uygunluk (fitness) değeri yüksek çözümler, bir sonraki nesle **daha yüksek olasılıkla** aktarılır.
- **Çaprazlama (Crossover)**: Ebeveyn çözümlerin parametrelerini birleştirerek yeni "bireyler" (çözümler) oluşturulur.
- **Mutasyon (Mutation)**: Yeni çözümlerin bir kısmında rastgele veya kontrollü bir değişiklik (pertürbasyon) eklenir; popülasyonda **çeşitlilik** korunur.

Pareto Tabanlı GA (örneğin **NSGA-II**, MOEA [32]):

- Tek bir fonksiyon yerine, **dominasyon** ilkesiyle (non-dominated sorting) "baskın olmayan" çözümler seçilir.
- Pareto çizgisi (Pareto front) üzerindeki çözümlerin çeşitliliğini korumak için **yoğunluk uzaklığı (crowding distance)** metriği kullanılır.
- Her nesilde, **domine olmayan** bireyler **elit koruma** ile saklanır, böylece aynı anda **min*T***, **min*E***, **max*P*** için farklı **denge noktaları** yakalanır.

2.3.2.3. Proje Kapsamında WOA ve GA

- **Parametre Vektörü**: Maskeleme parametreleri, Homomorfik şifreleme anahtar boyutu, MPC taraf sayısı, İletişim tur sayısı, Uç cihaz sayısı, Veri boyutu
- **Popülasyon / Balinalar**: WOA'da "balinalar" $\mathbf{x}_i$, GA'da "bireyler" $\mathbf{x}_i$.
- **Iterasyon / Nesil**: Her aşamada, çözümlerin (T,E,P) değerleri hesaplanır ve **dominasyon** analizine göre **Pareto front** güncellenir [32].

Çözüm uzayı genişse (örn. **bit boyutu, tur sayısı, maskeleme düzeyi** gibi yüzlerce değişken), **HPC sunucular** üzerinde **paralel** olarak WOA veya GA çalıştırılacaktır. Hız–kalite dengesi açısından, **her iki yöntem** de test edilip **karşılaştırmalı** analiz yapılması planlanmaktadır. Gerekirse, **ensemble** yaklaşımlar ([14,17]) da kullanılabilir (ör. WOA çıktısını GA'ya başlangıç popülasyonu yapma veya tersi) ve böylece **yerel minimumları aşma** şansı artar.

Dinamik Senaryolar ve Kısıtlar:

- Farklı senaryolarda (ör. **yüksek saldırı riski**) gizlilik metriği **P** için asgari bir eşik konabilir.
- **Düşük pil** koşullarında, enerji **E** üst limiti aşıldığında çözümler elenebilir.
- Bu tür **dinamik kısıtlar**, Pareto front'taki çözümler arasından pratikte hangilerinin seçileceğini belirleyecektir.

Sonuç olarak, **WOA** ve **GA**, proje bağlamında **çok amaçlı Pareto optimizasyon** yaklaşımıyla **federe öğrenme protokolleri** için **en uygun** parametre setlerini bulma hedefiyle kullanılacaktır. Farklı ağ koşulları, saldırı düzeyleri veya gecikme gereksinimleri gibi durumlarda **Pareto front** üzerinde **uygun** çözümler seçilebilecek; böylece **akıllı ve dinamik** bir parametre seçimi mekanizması oluşturulacaktır.

2.4. Prototip Geliştirme ve Uygulama

Bu aşamada, güvenli toplama protokolü modülleri Python/C++ üzerinde geliştirilecek, hem sanal hem de fiziksel test ortamları kullanılarak kapsamlı bir şekilde değerlendirilecektir. Uygulama ortamı üç ana bileşene ayrılacaktır:

1. **Prototip Mimarisi**

   - **Uç Cihazlar (Client):**

     - Arduino Tabanlı Kartlar: Düşük güçlü sensör ve veri toplama işlemleri için kullanılacaktır.
     - Raspberry Pi: Daha yüksek işlem gücü gerektiren uygulamalar için kullanılacak; IoT cihazlarının gerçek dünya senaryolarını benzetmek amacıyla işlevselliği artırılacaktır.
     - Bu cihazlar, farklı kriptografik parametrelerin (Maskeleme parametreleri, Homomorfik şifreleme anahtar boyutu, MPC taraf sayısı, İletişim tur sayısı, Uç cihaz sayısı, Veri boyutu) etkisini ölçmek amacıyla kontrol edilebilir şekilde yapılandırılacaktır.

   - **Sunucu (Aggregator / Koordinatör):**

     - HPC sunucusu veya bulut tabanlı platform, protokol modüllerinin entegrasyonunu ve koordinasyonunu sağlayacak; güvenli toplama işlemi ve Pareto optimizasyonu süreçlerinin merkezi yönetimi burada gerçekleştirilecektir.

   - **Ağ Katmanı:**

     - MQTT, TCP/IP veya benzeri iletişim protokolleri kullanılarak cihazlar arası veri alışverişi sağlanacaktır.
     - Ağ performansının gerçek zamanlı olarak izlenebilmesi için, iletişim tur sayısı ve veri boyutu gibi parametreler de kontrol altında tutulacaktır.

2. **Test Ortamları**

   - **Sanal Test Ortamı – ICSSIM:**
     - SCADA/PLC sistemlerini mikro hizmet tabanlı modelleyen ICSSIM, endüstriyel sensör verileri, sanal PLC'ler ve sistem parametrelerini içeren bir simülasyon ortamı sunacaktır.
     - Bu ortam, protokolün gerçek zamanlıya yakın verilerle test edilmesini ve iletişim, gecikme, enerji tüketimi ile protokol kararlılığı gibi metriklerin ölçülmesini sağlayacaktır.
   - **Fiziksel Benzetim Test Yatağı:**
     - Arduino ve Raspberry Pi Tabanlı Test Yatağı:
       - Gerçek donanım üzerinde, IoT cihazlarının işlevlerinin taklit edilmesi için Arduino ve Raspberry Pi kartları entegre edilecektir.
       - Bu test yatağı, laboratuvar ortamında kurulacak ve gerçek cihazlar üzerinden veri alışverişi, protokol uygulaması, dropout (cihazların geçici çevrimdışılığı) yönetimi gibi senaryoları canlandıracaktır.
     - Bu yapı sayesinde, sanal ortamdaki sonuçlarla fiziksel cihazlardaki performansın karşılaştırılması ve modelin gerçek dünya koşullarına adaptasyonu mümkün olacaktır.

3. **Metriklerin Ölçümü ve Değerlendirme**

   Prototipin performansı aşağıdaki metrikler üzerinden değerlendirilecektir:

   - **Gecikme (T):**

     - Şifreli veya maskeli veri transferi sırasında gerçekleşen iletişim gecikmesi (T_comm) ve işlem gecikmesi (T_comp) ölçülecektir.
     - Hem sanal ortamda (ICSSIM) hem de fiziksel test yatağında elde edilen ortalama tur süresi değerlendirilecektir.

   - **Enerji Tüketimi (E):**

     - Arduino ve Raspberry Pi gibi uç cihazlarda, protokol modüllerinin çalışması sırasında harcanan enerji, gerçek ölçüm cihazları veya yazılımsal tahmin kütüphaneleri kullanılarak hesaplanacaktır.

- İletişim ve işlem aşamalarında enerji tüketimi ayrı ayrı analiz edilecektir.

- **Gizlilik (P):**
  - Protokolün pasif ve aktif saldırı senaryolarında (örneğin, veri dinleme veya mesaj manipülasyonu) koruma seviyeleri değerlendirilecektir.
  - Kriptografik yöntemlerin (maskeleme, homomorfik şifreleme, MPC) entegrasyonu sonucunda, veri bütünlüğü ve gizlilik seviyeleri belirlenen ölçütler üzerinden incelenecektir.

- **Protokol Kararlılığı ve Dropout Yönetimi:**
  - Uç cihazların belirli turlarda çevrim dışı kalması durumunda protokolün nasıl esneklik sağladığı, dropout'a dayanıklı mekanizmaların işleyişi detaylı şekilde test edilecektir.
  - Hem simülasyon hem de fiziksel test ortamlarında, dropout durumlarında sistemin devamlılığı ve güvenlik sağlaması ölçülecektir.

Bu yapı, geliştirilen güvenli toplama protokolünün hem sanal hem de gerçek donanım koşullarında kapsamlı olarak test edilmesine olanak tanıyacak, ölçülen metrikler doğrultusunda sistemde gerekli iyileştirmelerin yapılmasını sağlayacaktır.

2.5. Performans Değerlendirme ve Yaygınlaştırma

Toplanan **maliyet** ve **performans** verileri, literatürdeki **yalnızca maskeleme** veya **yalnızca HE** gibi yöntemlerle karşılaştırılacaktır [14,15,27]. **Pareto tabanlı** sonuçlar, **%15 ve üzeri** öngörülen verimlilik kazançlarını (enerji ve gecikme boyutunda) teyit etmeyi amaçlar.

- **İstatistiksel Analiz**:
  - Tek yönlü ANOVA veya çoklu karşılaştırma testleri (Tukey, Bonferroni) kullanılarak, **farklı protokol konfigürasyonlarının** istatistiksel anlamlılığı incelenecektir.
  - Zaman serisi analiziyle, her turdaki gecikme T ve enerji E tüketiminin değişimi irdelenecektir [16,21].

- **Yaygınlaştırma**:
  - Akademik makaleler, konferans bildirileri ve sektörle yapılacak çalıştaylar yoluyla, **bilim topluluğuna** ve **endüstriyel paydaşlara** proje çıktıları aktarılacaktır [15,27].
  - **Pareto front** yapısı sayesinde, **farklı senaryolarda** elde edilen **değişik denge noktaları** da ortaya koyacakları sonuçlar kapsamında farklı bakış açıları ortaya koyabilir. Bu noktada ilgili paydaşlarla uygun yollar kullanılarak bu bilgiler de paylaşılacaktır.

Ek: Performans değerlendirmesinde yalnızca ortalama değerler değil, **ROC (Receiver Operating Characteristic), Precision-Recall, F1-score** gibi saldırı tespiti metrikleri de kullanılacaktır. Böylece **yanlış alarm** (False Positive) ve **atlanmış saldırı** (False Negative) oranları hakkında daha kapsamlı sonuçlar elde edilebilecektir.

2.6. Ön Çalışmalar ve Altyapı

Proje ekibinin lideri Doç. Dr. Oğuzhan Ceylan'ın **çok amaçlı optimizasyon** alanındaki deneyimi (örn. [16,17,20]) zaten bu projenin ön çalışmalarını teşkil etmektedir. Daha önce **dağıtık enerji sistemleri** ve **IoT kaynak ataması** konularında **WOA** ve **GA** yöntemlerinin verimli sonuçlar verdiği rapor edilmiştir. Ayrıca proje ekibi, Edge-IIoT veri seti kullanımı ve ICSSIM üzerinde **temel seviye test** deneyimlerine sahiptir. Dolayısıyla proje başlangıcında, gereksinim analizi tamamlandığında hızla protokol tasarımı ve pilot test aşamasına geçilebilecektir.

Özetle, yöntem bölümü; **araştırma tasarımının mantığını**, **bağımlı ve bağımsız değişkenleri**, **matematiksel modellemeyi**, **optimizasyon tekniklerini**, **prototip geliştirme** adımlarını ve **performans değerlendirmesi** kriterlerini kapsamlı biçimde açıklamaktadır. Bu yaklaşım, **proje amaç ve hedeflerine** ulaşmayı mümkün kılacak şekilde yapılandırılmıştır, zira her aşama bir öncekinden elde edilen girdilerle beslenmekte ve son aşamada **literatüre karşılaştırmalı** bir değerlendirme sunulmaktadır.

3. PROJE YÖNETİMİ

3.1. Yönetim Düzeni: İş-Zaman Çizelgesi ve İş Paketleri

Proje Ekibi: Prof. Dr. Hasan Dağ (Danışman), Doç. Dr. Oğuzhan Ceylan (Proje Yürütücüsü) – (İP 1,2,4), Doktora Bursiyeri 1 (D1) – (İP 2,3,4), Doktora Bursiyeri 2 (D2) – (İP 1,2), Yüksek Lisans Bursiyeri (YL1) – (İP 3,4), Lisans Bursiyeri 1 (L1) – (İP 1), Lisans Bursiyeri 2 (L2) – (İP 3)

3.1.1. İş-Zaman Çizelgesi

İŞ-ZAMAN ÇİZELGESİ (*)

İP No	İş Paketi Adı	Projenin Başarısındaki Önemi (%) (**)	Kim(ler) Tarafından Gerçekleştirileceği (***)	AYLAR																																			
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	Protokol Tasarımı ve Metodoloji Geliştirme	20	Y, D2, L1	X	X	X	X	X	X	X	X	X	X	X	X																								
2	Matematiksel Modelleme ve Optimizasyon	35	Y, D1, D2						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X												
3	Prototip Geliştirme ve Uygulama (Edge-IIoT, ICSSIM)	25	D1, YL1, L2																	X	X	X	X	X	X	X	X	X	X	X	X								
4	Performans Değerlendirme ve Yaygınlaştırma	20	Y, D1, YL1																					X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

3.1.2. İş Paketleri

<table>
<tr><th colspan="2">İŞ PAKETİ TABLOSU (*)</th></tr>
<tr><td>İP No: 1</td><td>İP Adı: Protokol Tasarımı ve Metodoloji Geliştirme</td></tr>
<tr><td colspan="2">İP Hedefi:

• Maskeleme, HE ve MPC tabanlı güvenli bir araya getirme protokol(ler)inin adım adım akışını tasarlamak.
• İletişim tur sayısı, dropout yönetimi ve anahtar değişimi gibi kritik detayları tanımlamak.
• Pasif/aktif saldırı senaryolarına karşı protokolün dayanıklılık analizini oluşturmak.</td></tr>
<tr><td>İP Kapsamında Yapılacak İşler/Görevler:

• Kriptografik yaklaşım(lar)ın (maskeleme+HE, MPC+maskeleme, ve diğer kombinasyonlar) şema çizimleri.

• Her protokolün haberleşme aşamalarının (uç cihazdan sunucuya, sunucudan uç cihaza) belirlenmesi.

• Dropout resilient (katılımcı uç cihazların bağlantı kesintisi) mekanizmasının tasarlanması.

• Güvenlik analizi: Pasif saldırılarda maskeleme çözülmesi, aktif saldırıda sahte parametre girişimi, vs.</td><td>İP'yi Gerçekleştirecek Kişi(ler) ve İP'ye Katkıları (**)

• Proje Yürütücüsü (Y): Genel metodolojinin ve protokol adımlarının ana hatlarını belirleme, güvenlik analizi için yönlendirme.
• Doktora Bursiyeri 2 (D2): Kriptografik yöntemlerin (örn. MPC, HE) taslaklarını oluşturma; SCADA/PLC uyumluluğu için teknik gereksinim analizi.
• Lisans Bursiyeri 1 (L1): Literatür taraması, küçük ölçekli deneme senaryoları (dropout, pasif saldırı) hazırlığı, akış diyagramları çizimi.</td></tr>
<tr><td colspan="2">Başarı Ölçütü: İlgili iş paketinin hangi kriterleri sağladığında başarılı sayılacağı ölçülebilir ve izlenebilir şekilde nitel ve/veya nicel olarak belirtilir.

• En az iki farklı güvenli protokol için ayrıntılı akış şeması ve metodoloji dokümantasyonu tamamlanacaktır.

• Pasif ve aktif saldırı türlerinin her birine (örneğin maskeleme çözümü, sahte parametre girişimi) karşı en az bir koruma stratejisi önerilecek ve raporlanacaktır.

• Küçük ölçekli konsept testlerinde, protokolün güvenli toplama işlevini en az %90 başarı oranıyla gerçekleştirdiği (örneğin veri bütünlüğünün korunması) gösterilecektir.</td></tr>
<tr><td colspan="2">Ara Çıktılar:

• Protokol Tasarım Dokümanı (akış diyagramları, UML benzeri şemalar).
• Pasif/aktif saldırı analiz raporu (farklı saldırı türlerine karşı dayanıklılık stratejileri).
• Konsept Test Sonuçları: Örneğin, küçük veri setiyle protokolün çalışıp çalışmadığını gösterir kısa rapor.</td></tr>
<tr><td colspan="2">Risk Yönetimi:</td></tr>
<tr><td>Risklerin Tanımı</td><td>Alınacak Tedbir(ler) (B planı)</td></tr>
<tr><td>• Protokolün çok karmaşık hâle gelmesi ve uygulamada zorlanma.</td><td>• Parçalı modüler tasarım, opsiyonel bileşenleri devre dışı bırakabilme (örneğin tam HE yerine kısmi HE kullanımı).</td></tr>
<tr><td>• Aktif saldırı senaryolarının eksik modellenmesi veya yeni/farklı tehditlerin proje sürecinde ortaya çıkması.</td><td>• Literatürdeki bilinen tüm tehdit modellerini gözden geçirmek. Yeni/farklı tehditlere için ek senaryolar belirlemek.</td></tr>
</table>

İŞ PAKETİ TABLOSU (*)

İP No: 2	**İP Adı:** Matematiksel Modelleme ve Optimizasyon

İP Hedefi:

- Her protokolün işlem süresi, bant genişliği, enerji maliyeti ve gizlilik düzeyi gibi parametrelerini matematiksel formüllerle ifade etmek.
- Her bir protokolün (T,E,P) metriklerine dayalı **çok amaçlı optimizasyon** modelini tanımlayıp, WOA ve GA gibi meta-sezgisel teknikler ile parametre uzayında **dominasyon ilkesi** üzerinden **Pareto front** araması yapmak.
- Optimizasyon sonuçlarını; elde edilen **enerji tasarrufu**, **iletişim gecikmesinde azalma** ve **gizlilik düzeyindeki iyileşme** gibi çıktılar üzerinden **istatistiksel olarak analiz etmek**.

İP Kapsamında Yapılacak İşler/Görevler:	**İP'yi Gerçekleştirecek Kişi(ler) ve İP'ye Katkıları (**)**
• Gecikme (T), enerji (E), gizlilik (P) metriklerine dair fonksiyonların oluşturulması. • T, E, P metriklerinin **birlikte** (çok amaçlı) optimize edileceği **Pareto** yaklaşımının tanımlanması; senaryoya bağlı **kısıtların** veya **önceliklerin** (ör. minimum gizlilik, maksimum gecikme) belirlenmesi. • Balina Optimizasyon Algoritması (WOA) ve Genetik Algoritma (GA) kodlarının uyarlanması veya geliştirilmesi. • HPC (Yüksek Performanslı) sunucular üzerinde ilk optimizasyon testlerinin yapılması.	• **Proje Yürütücüsü (Y):** Pareto-temelli çok amaçlı optimizasyon yaklaşımının seçimi ve genel çerçevesi; çıktıları doğrulama. • **Doktora Bursiyeri 1 (D1):** Balina Optimizasyon Algoritması (WOA) veya Genetik Algoritma (GA) kodlarını uyarlama, enerji-gizlilik gecikme fonksiyonlarını formüle etme. • **Doktora Bursiyeri 2 (D2):** HPC (yüksek performanslı hesaplama) üzerinde model çalışmaları, parametre ince ayarı ve istatistiksel analiz (ör. ANOVA, p değerleri).

Başarı Ölçütü: *İlgili iş paketinin hangi kriterleri sağladığında başarılı sayılacağı ölçülebilir ve izlenebilir şekilde nitel ve/veya nicel olarak belirtilir.*

- En az iki farklı optimizasyon algoritması (**örneğin WOA ve GA**) kullanılarak gerçekleştirilecek çok amaçlı optimizasyon sürecinde, **hedef kriterlerin** — enerji tüketimi, iletişim gecikmesi ve gizlilik düzeyi — **her biri için optimum değerin en az %80'ine ulaşılması** sağlanacaktır.
- Optimizasyon sonucunda, **enerji tüketimi** referans sistemle karşılaştırıldığında **en az %15 oranında azaltılacaktır**. Gecikme süresi, referans sisteme kıyasla en az %30 oranında düşürülecektir.
- Model doğruluğu %90'ın üzerinde korunacak ve elde edilen sonuçların $p < 0.05$ düzeyinde istatistiksel anlamlılığı gösterilecektir.

Ara Çıktılar:

- Matematiksel Model Dokümanı (E, T, P formülleri)
- Optimizasyon Algoritmaları Kaynak Kodu (Python/C++)
- Performans Raporu: Deneme senaryolarında en iyi/ortalama başarı değerleri, parametre kombinasyonları.

Risk Yönetimi:

Risklerin Tanımı	**Alınacak Tedbir(ler) (B planı)**
• HPC sunucuda yeterli hesaplama kaynağı bulunmaması veya gecikme yaşanması.	• Üniversitenin/iş birliği yapılan kurumların bulut altyapılarına veya ek HPC kaynaklarına başvurmak.

• Pareto front üretiminin yetersiz kalması (çok az sayıda domine olmayan çözüm elde etme).	• Parametre aralığını genişletmek, ek mutasyon/keşif adımlarıyla çeşitliliği artırmak.
• Optimizasyon algoritmalarının yerel minimuma takılması veya sonuçların çok uzun sürede yakınsamaması.	• Farklı meta-sezgisel yöntemler (PSO, Tabu Search) denemek, parametre ince ayarı yapmak.

İŞ PAKETİ TABLOSU (*)

İP No: 3	**İP Adı:** Prototip Geliştirme ve Uygulama (Edge-IIoT, ICSSIM)

İP Hedefi:

- Tasarlanan güvenli bir araya getirme protokol(ler)ini, Python/C++ ortamında, Edge-IIoT veri seti ve ICSSIM test yatağında çalışan bir prototipe dönüştürmek.
- Gecikme, bant genişliği, enerji tüketimi gibi metrikleri gerçekçi senaryolarda ölçmek.

İP Kapsamında Yapılacak İşler/Görevler:	**İP'yi Gerçekleştirecek Kişi(ler) ve İP'ye Katkıları (**)**
• Protokol modüllerinin (maskeleme, HE, MPC) yazılım geliştirmesi ve entegrasyonu. • Edge-IIoT veri setinde siber saldırı tespit senaryosu: Uç cihazların FL eğitimine katılımı, güvenli toplama protokollerinin uygulanması. • ICSSIM test yatağında endüstriyel kontrol senaryosu: SCADA/PLC verilerinin federe öğrenmeyle işlenmesi. • Fiziksel benzetim test yatağının oluşturuması ve yöntemin fiziksel ortamda uygulanması • Performans ölçümleri: Aktarılan veri boyutu, işlem süresi, enerji tüketimi (ör. Raspberry Pi üzerinde) gibi değerlerin kayıt altına alınması.	• **Doktora Bursiyeri 1 (D1):** Prototip yazılımın omurgasını hazırlama, Edge-IIoT veri seti entegrasyonunda optimizasyon modüllerini bağlama. • **Yüksek Lisans Bursiyeri (YL1):** Kod geliştirme (Python/C++), ICSSIM ortamında endüstriyel kontrol senaryosu kurma, enerji ve gecikme ölçümleri. • **Lisans Bursiyeri 2 (L2):** Kurulan yazılımların test otomasyonu, hata ayıklama; veri toplama ve raporlama (ör. performans grafikleri).

Başarı Ölçütü: *İlgili iş paketinin hangi kriterleri sağladığında başarılı sayılacağı ölçülebilir ve izlenebilir şekilde nitel ve/veya nicel olarak belirtilir.*

- Prototip, Edge-IIoT ve ICSSIM ortamlarında sorunsuz (%90 veya üzeri başarı ile) çalışacak şekilde devreye alınacaktır.
- En az iki senaryoda (ör. enerji ve saldırı tespiti) ortalama gecikmeyi %30, enerji tüketimini %15 oranında azaltması hedeflenecektir.
- Model doğruluğu %90'ın altında düşmeyecek şekilde 5 ila 10 tur arasında FL güncellemesini (dropout yönetimi dahil) hatasız tamamlaması sağlanacaktır.

Ara Çıktılar:

- Çalışan Prototip Yazılım (Python/C++ deposu)

• Test Sonuç Raporları (Edge-IIoT ve ICSSIM): Tablo ve grafiklerle performans değerlendirmesi. • Video veya Demo Kaydı (opsiyonel): Sunum için kısa bir prototip gösterimi.

Risk Yönetimi:

Risklerin Tanımı	**Alınacak Tedbir(ler) (B planı)**
• Edge-IIoT veri seti ve ICSSIM test yatağında beklenenden farklı hata mesajları veya yazılım uyumsuzlukları.	• Versiyon uyumluluk kontrolleri, ek dokümantasyon veya benzer veri seti/test ortamlarına geçiş (örn. siber saldırı veri setlerinde NSL-KDD, CICIDS).
• Yazılımda yüksek bellek veya CPU tüketimi.	• Kod ve algoritma optimizasyonu, daha hafif kriptografik kütüphaneler, HPC desteği.

İŞ PAKETİ TABLOSU (*)

İP No: 4	**İP Adı:** Performans Değerlendirme ve Yaygınlaştırma

İP Hedefi:

- Ortaya çıkan sonuçları literatürdeki benzer protokollerle karşılaştırarak, verimlilik kazanımını göstermek.
- Bilimsel makale ve bildiriler hazırlamak, sektörel iş birliklerini geliştirmek, olası patent başvurularını değerlendirmek.

İP Kapsamında Yapılacak İşler/Görevler:	**İP'yi Gerçekleştirecek Kişi(ler) ve İP'ye Katkıları (**)**
• Proje sonuçlarının analizi: Elde edilen ölçümler, optimizasyon başarıları, protokol verimliliği. • Literatürdeki protokollerle kıyas: Maskeleme, HE, MPC için tipik referans değerler (ör. Bonawitz protokoller [2]). • Bilimsel yayınlar: En az 2 SCI makale, uluslararası konferans bildirileri. • Sektörel iş birliği toplantıları, demo sunumları, muhtemel patent/faydalı model süreçlerinin başlatılması.	• **Proje Yürütücüsü (Y):** Literatürdeki referans yöntemlerle karşılaştırma, proje sonuçlarını akademik/sanayi paydaşlarına sunma, makale ve bildirileri koordine etme. • **Doktora Bursiyeri 1 (D1):** Elde edilen sonuçların analizinde (ör. enerji, gecikme, gizlilik) öne çıkan iyileştirmelerin yazılı hale getirilmesi, SCI makale taslakları hazırlığı. • **Yüksek Lisans Bursiyeri (YL1):** Yayınlarda kullanılacak grafik ve tablo derlemeleri, prototip demosu için teknik hazırlık, sektörel iş birliği sunumlarına destek.

Başarı Ölçütü: *İlgili iş paketinin hangi kriterleri sağladığında başarılı sayılacağı ölçülebilir ve izlenebilir şekilde nitel ve/veya nicel olarak belirtilir.*

- Geliştirilen protokol, literatürdeki benzer yaklaşımlara göre enerji tüketimi ve gecikme süresi bakımından en az %15–%30 arası iyileşme sağlayacaktır.
- İletişim yükü ve kriptografik hesaplama maliyetleri, mevcut referans protokollere kıyasla en az %20

azaltılacaktır. • Verimlilik kazanımı, teknik rapor ve karşılaştırma analizleriyle nicel olarak ispatlanacak ve sektörel/akademik paydaşlarla paylaşılacaktır.
Ara Çıktılar: • Karşılaştırma Raporu: Diğer protokollerle (ör. Bonawitz) yan yana performans değerlendirmesi. • Akademik Yayınlar (makale, bildiri): Hazırlanmış ve gönderilmiş versiyonlar. • Patent/Faydalı Model Başvuru Dosyası (uygunluğa göre).
Risk Yönetimi:

Risklerin Tanıml	**Alınacak Tedbir(ler) (B planı)**
• Deneysel sonuçların literatürde beklenen düzeyde iyileşme göstermemesi (ör. hedeflenen %15–30 kazanıma ulaşılamaması).	• Parametre ince ayarı, ek optimizasyon veya protokol basitleştirme adımları. Proje temel hedefine sadık kalarak kısmi iyileşme oranıyla dahi sonuçların yayımlanması.
• Sektörel paydaşlarla zamanlama/koordinasyon sorunu.	• Prototip demo günlerini üniversite bünyesinde düzenlemek, gerekirse uzaktan çevrimiçi demo.

3.2. Araştırma Olanakları

ARAŞTIRMA OLANAKLARI TABLOSU (*)

Altyapı/Ekipman Türü, Modeli (Laboratuvar, Makine-Teçhizat, vb.)	**Yer Aldığı Yürütücü/Katılımcı Kurum/Kuruluş**	**Projede Kullanım Amacı**
Yüksek Performanslı Masaüstü Bilgisayar	Kadir Has Üniversitesi	Veri işleme, sanal test yatağının oluşturulması, sanal ortamdaki deneyleri gerçekleştirilmesi

4. YAYGIN ETKİ

4.1. Öngörülen Çıktılar

Çıktı Türü	**Öngörülen Çıktı(lar)**	**Öngörülen Zaman Aralığı (*)**
Bilimsel/Akademik Çıktılar (Bildiri, Makale, Kitap Bölümü, Kitap vb.):	**En az 2 adet SCI/SCI-Expanded makale** hazırlanacak ve aşağıdaki dergiler hedeflenecektir: • *IEEE Transactions on Industrial Informatics*	12–36 ay

	• *Computers & Security (Elsevier)* • *Sensors (MDPI)* Bu makalelerde, **güvenli federe öğrenme** ile **çok kriterli optimizasyon** arasındaki ilişki ve **EKS/IoT senaryoları** detaylı biçimde ele alınacaktır. **En az 2 adet uluslararası konferans bildirisi** hazırlanarak, *IEEE/ACM* kapsamındaki güvenlik, IoT ve endüstriyel kontrol sistemleri alanındaki konferanslara (örn. Universities Power Engineering Conference, Smart Energy Systems and Technologies konferanslarına katılım, Uluslararası Bilgisayar Mühendisleri Konferansı, International Management Information Systems Conference) gönderilecektir. **Yurt içi/yurt dışı sempozyum sunumları** yapılacak ve proje sonuçları akademik ve sektörel paydaşlarla paylaşılacaktır.	
Ekonomik/Ticari/Sosyal Çıktılar (Ürün, Prototip, Patent, Faydalı Model, Üretim İzni, Tescil, Görsel/İşitsel Arşiv, Envanter/Veri Tabanı/Belgeleme Üretimi, Spin-off/Start- up Şirket vb.):	- Güvenli ve enerji-verimli federe öğrenme prototipi (Python/C++ tabanlı) - Olası patent veya faydalı model başvurusu (kriptografik protokol bileşenleri) - Elektrik dağıtım, otomasyon şirketleri gibi potansiyel sektör ortaklarıyla atölye/demolar düzenlenmesi	18–36 ay
Araştırmacı Yetiştirilmesi ve Yeni Proje(ler) Oluşturulmasına Yönelik Çıktılar (Yüksek Lisans/Doktora/Tıpta Uzmanlık/Sanatta Yeterlik Tezleri ve Ulusal/Uluslararası Yeni Proje vb.):	**-** Projede çalışan 1 doktora ve 1 yüksek lisans öğrencisinin tez çalışmalarının tamamlanması - Proje sonuçlarından hareketle AB Horizon Europe, EUREKA vb. uluslararası fonlara başvuru	24–36 ay, Proje Sonrası

4.2. Öngörülen Etkiler

4.2.1. Öngörülen Uygulama Alanları

Proje başarıyla uygulandığında, kritik altyapı sektöründeki (enerji, su dağıtımı, ulaşım vb.) EKS/IoT cihazların veri paylaşımı ve makine öğrenmesi süreçleri güvenli, düşük gecikmeli ve enerji tasarruflu hâle getirilebilir (Bkz. On İkinci Kalkınma Planı 3.2.3.6 Bilgi ve İletişim Teknolojileri, 3.5.2 Güvenlik Hizmetleri). Projenin doğrudan etkileneceği veya yararlanacağı/sunacağı kurumlar:

- **Elektrik Dağıtım Şirketleri:** SCADA sistemlerinde algılanan verilerin, güvenli federe öğrenmeyle gerçek zamanlı analizinin yapılması (ör. arıza/kesinti tespiti, siber saldırı önleme) (Bkz. Plan 3.2.2.2 Enerji; 3.5.2 Güvenlik Hizmetleri).

- **Otomasyon ve IoT Üreticileri:** Sensörlerinden gelen verinin prototipteki güvenli toplama modülleriyle işlenmesi ve bu sayede “veri gizliliği uyumlu” çözümlerin sunulması (Bkz. Plan 3.2.3.3 Bilim, Teknoloji ve Yenilik; 3.2.3.6 Bilgi ve İletişim Teknolojileri).

- **Kamu Kurumları (Enerji Bakanlığı, Ulaştırma Bakanlığı vb.):** Kritik altyapılarda siber güvenlik politikalarının belirlenmesinde proje çıktılarından referans alınması (Bkz. Plan 3.5.2 Güvenlik Hizmetleri).

- **Savunma ve Güvenlik Sektörü:** Stratejik tesislerde veriye dayalı karar verme süreçlerinde FL (Federe Öğrenme) kullanımı yaygınlaşırken güvenlik risklerini minimize etmek (Bkz. Plan 3.2.2.3 Savunma Sanayii; 3.5.2 Güvenlik Hizmetleri).

Bu noktada, **On İkinci Kalkınma Planı'nda yer alan "İleri imalat teknolojileri, dijital dönüşüm ve siber güvenlik ekosisteminin geliştirilmesi" hedefiyle** (Bkz. Plan 3.2.3.3, 3.2.3.6 ve 3.5.2) proje çıktıları örtüşmektedir. Türkiye'de kritik altyapılarda siber güvenlik önlemlerinin artırılması, yerli ve milli teknolojilerin geliştirilmesi hedefi doğrultusunda (Bkz. Plan 3.2.2.3, 3.2.3.3), bu projenin sağladığı güvenli federe öğrenme altyapısı önemli bir katkı sunabilecektir.

4.2.2. Sosyo-ekonomik/Kültürel Katkı

- **Yaşam kalitesi ve sivil güvenlik:** Proje, siber saldırıları erkenden algılayıp önleme mekanizmalarını güçlendireceği için, toplumsal ölçekte kesintisiz enerji, güvenli ulaşım ve temiz su arzı gibi hayati hizmetlerin korunmasına katkı sunar.

- **Ekonomik ve Çevresel Faydalar:** Enerji tüketiminde %15'a varan tasarruf öngörüsü, IoT cihazların pil ve bakım maliyetlerini azaltarak sürdürülebilir bir çerçeve yaratır. Böylece **temiz ve döngüsel ekonomi** prensipleri desteklenir.

- **İklim Değişikliği ile Mücadele:** Verimsiz veri transferlerini azaltan ve uçta veri işleme kapasitesini artıran federe öğrenme, yüksek miktarda enerji tüketen veri merkezlerine olan bağımlılığı kısmen hafifletebilir.

- **Eğitim ve Farkındalık:** Geliştirilecek prototipler ve yayınlar, **yaşam boyu öğrenme** ve **yükseköğretim** kurumlarında yeni ders ve araştırma projelerini tetikleyebilir. Üniversitelerin kontrol, bilgisayar, elektrik-elektronik, enerji bölümlerinde FL ve güvenlik konularında müfredat geliştirilmesi mümkün hâle gelebilir.

Tüm bu katkılar, On İkinci Kalkınma Planı'nda belirtilen **"dijital dönüşüm, siber güvenlik, yüksek katma değerli üretim, nitelikli iş gücü ve inovasyon"** eksenleriyle doğrudan ilişkilidir. Aynı zamanda "sivil güvenlik" ve "sürdürülebilir kalkınma" alanlarında da **ulusal politika** belgelerine katkı sağlayabilecektir.

4.3. Proje Sonuçlarının Yayılımı ve Bilim İletişimi Kapsamında Gerçekleştirilecek Faaliyet Planı

Hedef Kitle: *Proje sürecinde elde edilecek çıktı ve ulaşılacak sonuçlardan yararlanması öngörülen hedef kitlenin (akademisyenler, politika yapıcılar ve uygulayıcılar, özel sektör, bireyler, belirli yaş grupları vb.) kimler olduğu, ilgili hedef kitleye ulaşmak için nasıl bir yol izleneceği ve hedef kitlenin öngörülen yayılım faaliyetlerinden nasıl yararlanacağı belirtilir.*

- **Akademisyenler ve Araştırmacılar:**
  - Bilgisayar, elektronik, kontrol ve enerji mühendislikleri alanlarında çalışan akademisyenler.
  - Siber güvenlik ve yapay zekâ araştırma grupları, kriptografi uzmanları.
- **Politika Yapıcılar ve Uygulayıcılar:**
  - Bakanlıklar (Enerji, Ulaştırma, vb.), ilgili regülasyon kurumları.
  - Yerel yönetimler (akıllı şehir projeleri), kritik altyapı yöneticileri.
- **Özel Sektör ve Endüstri Temsilcileri:**
  - Elektrik dağıtım şirketleri, otomasyon firmaları, IoT üreticileri.
- **Genel Kullanıcılar ve Eğitim Kurumları:**
  - Veri gizliliğine önem veren bireyler, siber güvenlik farkındalığını arttırmak isteyen kitleler.
  - Lisans ve lisansüstü öğrenciler.

Hedefler ve Beklenen Kazanımlar:

- **Farkındalığın Artırılması:** Kritik altyapılarda güvenli federe öğrenmenin önemini vurgulamak, kamuoyunda ve sektörde **"veri mahremiyeti + yapay zekâ"** kavramına yönelik bilinci yükseltmek.
- **Bilgi Birikiminin Paylaşımı:** Akademik makale ve bildiriler, sektörel eğitimler, çalıştaylar aracılığıyla proje sonuçlarını aktarmak. Böylece **nitelikli insan kaynağı** yetişmesine destek olunması.
- **Teknoloji Transferi:** Prototip ve patent/faydalı model çalışmalarıyla, özel sektörde **ticari ürünleşme** ve **Ar-Ge iş**

birlikleri.

- **Politika Gelişimine Katkı:** Proje sonucunda ortaya çıkan bulguların, On İkinci Kalkınma Planı'nda yer alan **dijital dönüşüm** ve **siber güvenlik** hedeflerine yönelik politika tasarımlarına veri sağlaması.

Kullanılacak Araçlar:

- **Bilimsel Etkinlikler:** Konferans, seminer, atölye çalışmaları, çalıştaylar. Ulusal ve uluslararası kongrelerde sözlü/poster sunumlar.
- **Medya ve Yayınlar:** Ulusal/yerel basın için röportaj ve haber bültenleri, akademik dergilerde makaleler, endüstri dergilerinde popüler yazılar.
- **Sektörel Buluşmalar:** Fuarlar, endüstri günleri, demo veya pilot gösterimler. Prototipin gerçek donanım ortamlarında denenmesi.

Zamanlama: *Planlanan faaliyetlerin hangi zaman diliminde gerçekleştirileceği ve ne kadar süreceği açıklanır.*

- **0–6 ay:** Proje web sitesi, sosyal medya hesaplarının oluşturulması, basit tanıtım materyalleri (infografikler, posterler).
- **6–12 ay:** İlk literatür raporu ve tasarım bulguları yayınlanır; sektörel paydaşlarla pilot görüşmeler.
- **12–24 ay:** Prototipin ilk sürümü tamamlanır, **ulusal/uluslararası konferans** bildirileri sunulur. Akademik makale taslakları hazırlanır.
- **24–36 ay:** Nihai prototip testleri, patent/faydalı model başvurusu değerlendirmesi, **geniş katılımlı çalıştay** veya demo günleri. Makalelerin son hali yayımlanır.
- **Proje Sonrası:** Spin-off/start-up imkânları, yeni proje başvuruları (AB Horizon Europe, TEYDEB vb.), endüstriyel iş birliği geliştirme.

BELİRTMEK İSTEDİĞİNİZ DİĞER KONULAR

BAŞVURU FORMU EKLERİ

EK-1: KAYNAKLAR

EK-2: BÜTÇE VE GEREKÇESİ

EK-3: PROJE EKİBİNİN DİĞER PROJELERİ VE GÜNCEL YAYINLARI (Proje Başvuru Sistemi (PBS)'ne girilen bilgiler doğrultusunda Sistem tarafından otomatik olarak oluşturulmaktadır.)