[1] Bu makalede araştırmacılar yaptıkları çalışmada ağ altyapılarının artan karmaşıklığı karşısında geleneksel manuel ağ yönetimi ve olay müdahale yöntemlerinin yetersizliğini ele almışlardır. Araştırmacılar verimliliği, güvenliği ve performansı artırmak amacıyla yapay zeka, makine öğrenimi ve yazılım tanımlı ağ (SDN) kullanarak bu işlevlerin otomasyonunu keşfetmeyi amaçlamışlardır.

Araştırmada nitel ve nicel yöntemleri birleştiren karma bir yaklaşım benimsemişlerdir. Ağ yöneticilerinden nicel veriler anket yardımıyla toplanmış, sektör uzmanlarıyla yapılan yarı yapılandırılmış röportajlar ile nitel bilgiler almışlardır. Bulguları doğrulamak için deneysel bir ağ ortamı oluşturmuşlardır. Nitel verileri tematik analizle, nicel verileri ise tanımlayıcı ve çıkarımsal istatiksel yöntemlerle analiz etmişlerdir. Otomatik sistemlerin verimliliğini değerlendirmek için ortalama çözüm süresi (MTTR), ağ kesinti süresi ve olay tespit oranları gibi metrikler kullanmışlardır.

Otomasyonun, ağ yönetimi ve olay müdahalesinde önemli faydalar sağladığını ortaya koymuşlardır. Manuel müdahaleyi azaltarak ve proaktif ayarlamalarla ağ performansını optimize edip, verimliliği artırmışlardır. ML algoritmaları kullanarak şüpheli etkinlikleri gerçek zamanlı olarak izleyerek ve tehditleri hızla azaltarak güvenliği artırmayı başarmışlardır. Sonuç olarak otomasyonun verimlilik, güvenlik ve maliyet tasarrufu açısından önemli iyileştirmeler sağladığı vurgulanmıştır.

[2] Bu makalede araştırmacılar ağ güvenliği yönetiminde güvenlik denetiminin karşılaştığı temel sorunları analiz etmeyi ve bu sorunlara yönelik çözümler önermeyi amaçlamışlardır. Belirlenen sorunları şu şekilde belirtmişlerdir;

* Büyük miktarda veriyi işlemenin karmaşıklığı,
* Denetim teknolojileri ve araçlarının yetersizliği,
* Hem personel hem de kuruluşlar arasındaki güvenlik farkındalığının zayıflığı.

Makalede, doğrudan teknik uygulama yerine, güvenlik denetiminin karşılaştığı zorlukları ele almak için teknolojik yenilikler, süreç iyileştirmeleri ve personel yeterliliklerinin artırılması gibi stratejileri önerilmiştir. Ağ Güvenliği Politikası Yönetimi (NSPM) ve otomasyonun rolü de vurgulanmıştır. Güvenlik denetiminin rolünün artırılmasına yönelik olarak, hızla değişen ve gelişen Yapay Zeka ve Makine Öğrenmesi teknolojilerinin entegre edilmesinin uygulamanın daha verimli, anomali tespitinde daha güvenli ve esnekilik sağlayabileceği belirtilmiştir.

Araştırmacılar bu sorunlar ve öneriler ışığında şu çözümleri uygulamanın etkili olacağını savunmuşlardır;

* Denetim teknolojilerinde yenilik,
* Denetim süreçlerinin iyileştirilmesi ve otomasyonun entegrasyonu,
* Personel niteliklerinin ve güvenlik farkındalığının artırılması.

Sonuç olarak, artan güvenlik riskleri, verinin yönetilmesinin karmaşıklaşması ve teknolojik gelişmelerdeki açıklıklar-eksiklikler bu zorluklarla başa çıkmada etkili yöntemlerin uygulanmasını zorunlu kılmaktadır. Güçlü bir saha araştırması, personel farkındalığının artırılması, gerçek zamanlı performans ve denetim araçlarının ağa entegresi ile önemli ölçüde iyileşme sağlanması mümkün olmaktadır.

[3] Bu çalışmada araştırmacılar gelişen internet ağları ve iletişim sistemleri nedeniyle BT profesyonelleri için bir zorluk olan ağ altyapılarında etkili anomali tespit sistemlerine olan kritik ihtiyacı ele almışlardır. Temel amaçları, ağ trafiği verilerindeki nokta anomalilerini tespit etmek için Yapay Zeka algoritmaları tasarlamak ve uygulamak, anormal kalıpları ve davranışları tanımlayabilen bir sistem geliştirmek olmuştur. Araştırmacılar gerçek dünya koşullarını simüle etmek için sanal bir ağ ortamı tasarlanmıştır. Bant genişliği, verim, gecikme, titreşim, tıkanıklık ve paket kaybı gibi parametreleri ölçmek için Python ile özel bir ağ probu geliştirmişlerdir. Bu ortamdan toplanan veriler normalleştirilmiş ve temel özellikler çıkarılmıştır. Makine öğrenimi için hem denetimli hem de denetimsiz makine öğrenimi modelleri uygulanmış ve karşılaştırılmıştır;

* **Denetimsiz Öğrenme Modelleri:** Zaman serisi verilerindeki ani değişiklikleri tespit etmek için Değişim Noktası Tespiti ve farklı uzunluklardaki dizileri etkili bir şekilde hizalamak için Dinamik Zaman Bükme ile k-ortalama kümeleme kullanmışlardır.
* **Denetimli Öğrenme Modelleri:** Anomaliler; Lojistik Regresyon, Rastgele Orman ve Destek Vektör Makinesi (SVM) modelleri değerlendirmişlerdir.

Performans, doğruluk, kesinlik, geri çağırma ve F1-skoru gibi metrikler kullanılarak ölçmüşlerdir. Model yorumlanabilirliğini artırmak için Shapley Additive exPlanations (SHAP) değerleri kullanmışlardır.

Çalışma sonucunda önemli bulgular elde edilmiştir. Denetimsiz modellerde, zamansal kalıpları etkili bir şekilde yakalamış ve değişim noktalarını tespit etmişlerdir. Verim için, değerler düşük aralıklara (0-2 Mbps) düştüğünde CPs(Değişim Noktası Tespiti – Change Detection Point) tespit edilmiştir. Paket kaybı için, kümeleme yöntemi %20’yi aşan ciddi anomalileri tanımlamıştır. Denetimli modellerde, Lojistik regresyon **%91.2** doğruluk elde etmişlerdir, ancak karmaşık doğrusal olmayan ilişkileri yakalamada sınırlamalar göstermiştir. Rastgele Orman, doğruluğu **%94.3**’e yükseltmiştir. Veri karmaşıklıklarını daha iyi yakalamış ve gerçek anomali oranına daha yakın sonuçlar vermiştir. SVM, **%96.5** ile en yüksek doğruluğu elde etmiştir, ancak %6’lık yanlış pozitif oranıyla anomalileri biraz fazla tahmin etmiştir.

# KAYNAKÇA

|  |  |
| --- | --- |
| [1] | D. J. A. Smith, "Automation of Network Management and Incident Response," *SSRN Electronic Journal,* vol. 15, no. 16, 2020. |
| [2] | W. Sijun and Y. Dai, "Key Issues and Solutions of Security Auditing in Network Security Management," *PiscoMed,* vol. 14, no. 1, 2025. |
| [3] | P. Schummer, A. D. Rio, J. Serrano, D. Jimenez, G. Sanchez and A. Llorente, "Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation," *MDPI,* 2024. |