ÖZET

ANOMALİ İÇEREN DURUMLAR İÇİN DÜZELTME NOTU OLUŞTURULMASINI SAĞLAYAN BİR SİSTEM

Bu buluş, dijital ortamda tespit edilen anomali durumlarının ve açık kaynak verilerinin ilişkilendirilmesini, otomatik olarak bir not oluşturulmasını, oluşturulan notun veri sahibine gönderilmesini sağlayan bir sistem (1) ile ilgilidir.

İSTEMLER

1. Dijital ortamda tespit edilen anomali durumlarının ve açık kaynak verilerinin ilişkilendirilmesini, otomatik olarak bir not oluşturulmasını, oluşturulan notun veri sahibine gönderilmesini sağlayan;

- anomali durumlarını tespit etmek ve anomaliye ilişkin alarm oluşturmak üzere yapılandırılan en az bir anomali tespit modülü (2),
- açık kaynak kodlu yazılımlardan veri toplamak ve veri depolamak üzere yapılandırılan en az bir veri toplama modülü (3) içeren ve
- anomali tespit modülü (2) ve veri toplama modülü (3) çıktıları arasında ilişki kurmak üzere yapılandırılan en az bir veri işleme modülü (4),
- veri işleme modülü (4) çıktılarını alarak anomaliye ilişkin bir not üretilip üretilmeyeceğine ilişkin karar almak ve not oluşturulan durumda kullanıcıya ilgili notu görsel olarak iletmek üzere yapılandırılan en az bir sunucu (5) ile karakterize edilen bir sistem (1).

2. Web sayfaları, uygulamalar gibi dijital ortamlarda yer alan veriler üzerinde analiz yaparak önceden belirlenmiş verilerle uyumsuz olan veri varlığı durumlarının saptanmasını sağlamak üzere yapılandırılan anomali tespit modülü (2) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

3. Makine öğrenimi algoritmaları kullanarak tespit edilen anomali durumlarına ilişkin alarm oluşturmak üzere yapılandırılan anomali tespit modülü (2) ile karakterize edilen İstem 1 veya 2'deki gibi bir sistem (1).

4. Açık kaynak kodlu web sayfaları, uygulamalar gibi dijital ortamlarda yer alan verileri toplamak ve depolamak üzere yapılandırılan veri toplama modülü (3) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

5. Anomali tespit modülü (2) ve veri toplama modülü (3) ile iletişim halinde olup, yapay zeka algoritmaları vasıtasıyla anomali tespit modülü (2) ve veri toplama modülü (3) çıktıları arasında ilişki kurmak üzere yapılandırılan veri işleme modülü (4) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

6. Veri işleme modülü (4) ile iletişim halinde olup, veri işleme modülü (4) tarafından belirlenen ilişki doğrultusunda not oluşturulup oluşturulmayacağına yapay zeka algoritmaları vasıtasıyla karar vermek üzere yapılandırılan sunucu (5) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

7. Not oluşturulmasına karar verdiği durumda, anomali tespit modülü (2) üzerinden görsel veri almak, aldığı görsel verileri görüntü işleme algoritması ile işlemek ve görsel not oluşturarak söz konusu notu yetkili kullanıcıya iletmek üzere yapılandırılan sunucu (5) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

TARİFNAME

ANOMALİ İÇEREN DURUMLAR İÇİN DÜZELTME NOTU OLUŞTURULMASINI SAĞLAYAN BİR SİSTEM

Teknik Alan

Bu buluş, dijital ortamda tespit edilen anomali durumlarının ve açık kaynak verilerinin ilişkilendirilmesini, otomatik olarak bir akıllı düzeltme notu (smart annotation) oluşturulmasını, oluşturulan notun veri sahibine gönderilmesini sağlayan bir sistem ile ilgilidir.

Önceki Teknik

Günümüzde web sayfaları, uygulamalar ve yazılımlar üzerindeki verilerde meydana gelen beklenmedik durumları tespit eden çeşitli çalışmalar bulunmaktadır. Söz konusu çalışmalarda toplanan verilerin önceden tanımlanan ve beklenen verilerle uyumlu olup olmadığı analiz edilmektedir. Analiz sonucunda beklenen normal değerler dışında bir değere/özelliğe sahip veriler anomali olarak adlandırılmaktadır. Söz konusu çalışmalarda makine öğrenimi ve istatistik temelli tespit yöntemleri kullanılabilmektedir. Ancak kimi zaman anomali durumlarının tespit edilmesi, gerekli aksiyonun alınması için yeterli olmamaktadır. Anomali durumunda ilgili kullanıcıların aksiyon alabilmeleri için son kullanıcının anomali durumunu fark etmesinden önce düzeltme notu oluşturulmasını sağlayan çalışmalar mevcut teknikte yer almamaktadır.

Mevcut teknikte bulunan çalışmalar göz önünde bulundurulduğunda anomali durumları son kullanıcı tarafından fark edilmeden önce anomaliye ilişkin bir not oluşturulmasını ve oluşturulan notun veri sahibine/yetkili kullanıcıya iletilmesini sağlayan bir sisteme ihtiyaç duyulduğu anlaşılmaktadır.

Tekniğin bilinen durumunda yer alan US20020038430 sayılı Birleşik Devletler patent dokümanında siber tehlikelerin önceden tespit edilerek kullanıcıların bilgilendirilmesini sağlayan bir sistemden bahsedilmektedir. Söz konusu buluşta birçok kaynaktan siber tehlikelere ilişkin veri toplanmakta ve toplanan veri, analistin denetimine sunulmak üzere ön işlemden geçirilmektedir. Ön işlemden geçirilen veri, analist tarafından denetlenmekte ve kullanıcıları bilgilendirmek için alarm oluşturulmasına gerek olup olmadığına karar vermektedir. Buluş konusu sistem, toplamış olduğu verileri yeniden formatlamakta, derlemekte ve çeşitli iletim yöntemleri ile otomatik olarak iletmektedir. Buluş bir uygulamasında veri toplamak için çeşitli İnternet siteleri, e-posta dağıtım listeleri ve e-posta yönetim sistemleri, Usenetler, sohbet odaları diyalogları, devlet dokümanları gibi kaynaklar kullanılmaktadır. Toplanan veriler klavye aramasına, model eşleşmesine ve içerik tanıma işlevlerine göre filtrelenmekte ve kategorilerine ayrılmaktadır. Buluş konusu sistemde önceden tanımlanmış bir alıkoyma kriteri doğrultusunda veri filtrelemesi gerçekleştirilmektedir. Filtreleme ve kategorilere ayrılma işleminden sonra veriler sıraya sokulmaktadır ve bir analist tarafından sırayla incelenmektedir. Analist verileri etiketleyerek depolamaktadır ve kıdemli analist tarafından son karar verilmektedir. Kıdemli analistin kararı doğrultusunda kullanıcıya siber tehlike arz eden bilginin son biçimi oluşturulmakta ve iletilmektedir.

Buluşun Kısa Açıklaması

Bu buluşun amacı, anomali tespiti yapılmasını ve anomaliye ilişkin alarm oluşturulmasını sağlayan bir modül ve bir açık kaynak veri havuzundan alınan verilerin yapay zeka ile karar alan bir mekanizmada işlenmesiyle anomali durumuna ilişkin görsel bir notun otomatik oluşturulmasını ve kullanıcıya iletilmesini sağlayan bir sistem gerçekleştirmektir.

Buluşun Ayrıntılı Açıklaması

Bu buluşun amacına ulaşmak için gerçekleştirilen" Anomali İçeren Durumlar İçin Düzeltme Notu Oluşturulmasını Sağlayan Bir Sistem" ekli şekilde gösterilmiş olup, bu şekil;

Şekil-1; Buluş konusu sistemin şematik bir görünüşüdür.

Şekillerde yer alan parçalar tek tek numaralandırılmış olup, bu numaraların karşılıkları aşağıda verilmiştir.

1. Sistem
2. Anomali tespit modülü
3. Veri toplama modülü
4. Veri işleme modülü
5. Sunucu

Buluş konusu dijital ortamda tespit edilen anomali durumlarının ve açık kaynak verilerinin ilişkilendirilmesini, otomatik olarak bir not oluşturulmasını, oluşturulan notun veri sahibine gönderilmesini sağlayan bir sistem (1);

- anomali durumlarını tespit etmek ve anomaliye ilişkin alarm oluşturmak üzere yapılandırılan en az bir anomali tespit modülü (2),
- açık kaynak kodlu yazılımlardan veri toplamak ve veri depolamak üzere yapılandırılan en az bir veri toplama modülü (3),
- anomali tespit modülü (2) ve veri toplama modülü (3) çıktıları arasında ilişki kurmak üzere yapılandırılan en az bir veri işleme modülü (4),
- veri işleme modülü (4) çıktılarını alarak anomaliye ilişkin bir not üretilip üretilmeyeceğine ilişkin karar almak ve not oluşturulan durumda kullanıcıya ilgili notu görsel olarak iletmek üzere yapılandırılan en az bir sunucu (5) içermektedir.

Buluş konusu sistemde (1) yer alan anomali tespit modülü (2) web sayfaları, uygulamalar gibi dijital ortamlarda yer alan veriler üzerinde analiz yaparak önceden

belirlenmiş verilerle uyumsuz olan veri varlığı durumlarının saptanmasını sağlamak üzere yapılandırılmaktadır. Anomali tespit modülü (2) makine öğrenimi algoritmaları kullanarak tespit edilen anomali durumlarına ilişkin alarm oluşturmak üzere yapılandırılmaktadır.

Buluş konusu sistemde (1) yer alan veri toplama modülü (3) açık kaynak kodlu web sayfaları, uygulamalar gibi dijital ortamlarda yer alan verileri toplamak ve depolamak üzere yapılandırılmaktadır.

Buluş konusu sistemde (1) yer alan veri işleme modülü (4) anomali tespit modülü (2) ve veri toplama modülü (3) ile iletişim halinde olup, yapay zeka algoritmaları vasıtasıyla anomali tespit modülü (2) ve veri toplama modülü (3) çıktıları arasında ilişki kurmak üzere yapılandırılmaktadır.

Buluş konusu sistemde (1) yer alan sunucu (5) veri işleme modülü (4) ile iletişim halinde olup, veri işleme modülü (4) tarafından belirlenen ilişki doğrultusunda not oluşturulup oluşturulmayacağına yapay zeka algoritmaları vasıtasıyla karar vermek üzere yapılandırılmaktadır. Sunucu (5) not oluşturulmasına karar verdiği durumda, anomali tespit modülü (2) üzerinden görsel veri almak, aldığı görsel verileri görüntü işleme algoritması ile işlemek ve görsel not oluşturarak söz konusu notu yetkili kullanıcıya iletmek üzere yapılandırılmaktadır.

Bu temel kavramlar etrafında, buluş konusu sistem (1) ile ilgili çok çeşitli uygulamaların geliştirilmesi mümkün olup, buluş burada açıklanan örneklerle sınırlandırılamaz, esas olarak istemlerde belirtildiği gibidir.

Şekil 1