BDDK Bankacılık ve Finansal Piyasalar
Journal of BRSA Banking and Financial Markets
Cilt / Volume: 18
Sayı / Issue: 2
Yıl / Year: 2024
e-ISSN: 1307-945X
Araştırma Makalesi
Research Article

Bankacılık Sektöründe Bulanık HTEA Yöntemi Kullanılarak Bilgi Güvenliğinde Risk Analizi

Yıldız Merve YEŞİLÇİMEN*
Özlem Müge TESTİK**

Öz

İnternet ve bilişim teknolojilerinin hızla gelişmesi, kurumların iş süreçlerinde bilişim sistemlerine olan bağımlılıklarını artırarak onları bilgi teknolojisi tehditlerine karşı daha savunmasız hale getirmektedir. Bu durum, kurumların bilgi güvenliği risklerini etkili bir şekilde yönetmesini ve güvenilir kurum imajını koruyarak iş sürekliliğini sağlamasını gerektirmektedir. Bilgi güvenliğindeki riskleri belirlemek ve önlemek amacıyla bu makalede Hata Modu ve Etkileri Analizi (HTEA) yöntemi bulanık yaklaşımla birlikte sunulmaktadır. Bulanık HTEA; klasik HTEA'ya göre daha pratik ve esnek bir risk değerlendirme yöntemi olarak tercih edilmiştir. Çalışmanın amacı; bir kurumda taşınabilir ortam ve cihazlardaki bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik unsurlarında ortaya çıkabilecek riskleri belirleyerek, bu riskleri önleyici veya etkilerini azaltıcı çözümler sunmaktır. Çalışmada, bilgi güvenliği alanında uzman 7 kişilik bir ekiple çalışılmıştır. Hata modları belirlenirken Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanmış olan Bilgi ve İletişim Güvenliği Rehberi'nde yer alan 'Taşınabilir Cihaz ve Ortam Güvenliği' başlığındaki tedbir maddelerinden yararlanılmış ve 21 adet hata modu belirlenmiştir. Hata modlarının olasılık, şiddet ve tespit edilebilirlik parametreleri uzmanlar tarafından 10 farklı dilsel ölçekte değerlendirilmiştir. Aykırı değerlerin elimine edilmesi amacıyla medyan ile hesaplamalar yapılmıştır. Klasik ve Bulanık HTEA karşılaştırılması yapılarak iki yöntemin arasında güçlü bir uyum olduğu ancak Bulanık HTEA'nın daha esnek ve pratik olduğu sonucuna ulaşılmıştır.

Anahtar Kelimeler: Bilgi Güvenliği, Risk Analizi, HTEA, Bulanık HTEA.

JEL Sınıflandırması: M15, D81, C44.

Abstract - Using the Fuzzy FMEA Method Risk Analysis in Information Security

The rapid development of the Internet and information technologies increases the dependence of organizations on information systems in their business processes, making them more vulnerable to information technology threats. In light of these circumstances, it is imperative for organisations to proactively manage information security risks and ensure business continuity by maintaining a reliable and trustworthy corporate image. In order to identify and prevent risks in information security, this paper presents the Failure Mode and Effect Analysis (FMEA) method with a fuzzy approach. Fuzzy FMEA is preferred as a more practical and flexible risk assessment method than classical FMEA. The aim of the study is to identify the risks that may arise in the confidentiality, integrity and accessibility elements of information security in portable media and devices in an organization and to provide solutions to prevent or mitigate these risks. The study was conducted with a team of 7 experts in the field of information security. While determining the failure modes, the precautionary items under the heading 'Portable Device and Media Security' in the Information and Communication Security Guide prepared by the Digital Transformation Office of the Presidency of the Republic of Turkey were utilized and 21 failure modes were determined. The probability, severity and detectability parameters of the error modes were evaluated by experts on 10 different linguistic scales. In order to eliminate outliers, calculations were made on the median. Classical and Fuzzy FMEA were compared and it was concluded that there is a strong agreement between the two methods, but Fuzzy FMEA is more flexible and practical.

Keywords: Information Security, Risk Analysis, FMEA, Fuzzy FMEA.

JEL Classification: M15, D81, C44..

* Sorumlu Yazar, Bankacılık Düzenleme ve Denetleme Kurumu, İstanbul Teknik Üniversitesi İşletme Mühendisliği Doktora Öğrencisi - E-posta: myesilcimen@bddk.org.tr - ORCID: 0009-0009-6305-3867.
** Hacettepe Üniversitesi, Endüstri Mühendisliği Bölümü - E-posta: ozlemaydin@hacettepe.edu.tr - ORCID: 0000-0003-4451-0902.
Makale Gönderim Tarihi: 30.10.2024 Makale Kabul Tarihi: 29.11.2024
Atıf: Yeşilçimen, Y. M. ve Testik, Ö. M. (2024). Bankacılık Sektöründe Bulanık HTEA Yöntemi Kullanılarak Bilgi Güvenliğinde Risk Analizi. *BDDK Bankacılık ve Finansal Piyasalar Dergisi,* 18(2), 170-185.
http://doi.org/10.46520/bddkdergisi.1600281.

1. Giriş

Kurumların; müşteri bilgileri, finansal veriler ve ticari sırlar gibi hassas bilgileri içeren taşınabilir cihazlarını; yetkisiz erişimden, veri kaybından ya da değiştirilmesinden koruması kritik öneme sahiptir. İş süreçlerinde dijitalleşmenin hızla arttığı bu dönemde; taşınabilir cihazların bilgi güvenliği, kurumların sürdürülebilirliği, yasal uyumluluk ve itibarını koruma açısından hayati öneme sahiptir. Devlet seviyesinde ise stratejik bilgilerin güvenliği, ulusal güvenlik açısından oldukça önemlidir. Bilginin korunması, bireyler ve kurumların yanı sıra toplumun genel güvenliği ve istikrarı için de kritik olup; bilgi güvenliği önlemleri veri bütünlüğü sağlama, yetkisiz erişimi önleme ve erişim kontrolünü sağlamayı amaçlamaktadır. Bankacılık sektörü gibi yüksek risk içeren ve çeşitli regülasyonlara tabi olan alanlarda risklerin doğru analizi, iş sürekliliğinin ve güvenilirliğin sağlanması açısından önemli bir gerekliliktir.

İşletmeler, doğası gereği her zaman risk barındırmaktadır. Riskler belirlenmeli, yönetilmeli ve kabul edilebilir düzeye indirgenmelidir (Bidgoli, 2006). Bilgi güvenliğinde risk analizi ise, potansiyel ihlalleri zarar derecelerine göre önceliklendirerek Bilgi Teknolojileri (BT) kaynaklarını en verimli şekilde kullanmayı amaçlamaktadır (Shaikh ve Siponen, 2023). Geçmişte güvenilirliği artırmak amacıyla test ve analiz yöntemlerine başvurulurken, günümüzde bu yöntemlerin maliyetlerinin fazlasıyla yüksek olabilmesi nedeniyle tasarımın erken safhalarında güvenilirliğin sağlanması hedeflenmektedir. Hataların erken safhalarda öngörülebilmesi ve önlenebilmesi için Hata Modu ve Etkileri Analizi (HTEA-Failure Mode And Effect Analysis) en sık uygulanan analiz araçlarından biridir (Yang v.d., 2008; Carlson, 2012).

Bu çalışmada, bankacılık sektöründe taşınabilir cihaz ve ortamlardaki bilgi güvenliği risklerini minimize etmek ve etkili bir yaklaşım sunmak amacıyla HTEA kullanılmıştır. Ancak, HTEA yönteminde uzmanlardan alınan görüşler uzmanın alan bilgisi, tecrübesi ve kişisel görüşü nedeniyle subjektiflik içerebilmektedir. Bu subjektifiğin süreci olabilecek en az seviyede etkileyebilmesi amacıyla, klasik HTEA yöntemine bulanık mantık dahil edilerek analizlerde bulanık HTEA yönteminden yararlanılmıştır. Bu makale, bankacılık sektöründe taşınabilir cihaz ve ortamlarda bilgi güvenliği risklerini belirlemek ve bu alandaki riskleri önlemek için stratejiler geliştirmek isteyen araştırmacılar ve profesyoneller için bir kaynak sunmaktadır. Hata modları belirlenirken yararlanılan Bilgi Güvenliği Rehberinin gerçek dünya uygulamalarına entegrasyonu, yöntemlerin genişletilebilirliği ve farklı sektörlerdeki uygulanabilirliği konusunda literatüre bir katkı sunmayı hedeflemektedir.

2. Literatür

Chiozza ve Ponzetti (2009), laboratuar ortamlarında tıbbi hataların azaltılarak hasta güvenliğinin artırılması ve maliyet tasarrufu sağlanmasına yönelik HTEA risk analiz çalışmasını bir hastanede test ederek başarıya ulaştıklarını gözlemlemişlerdir. Kim v.d. (2013), akıllı telefonlardaki hata modlarının sebebinin güvenlik sistemleriyle alakalı yazılımlardan kaynaklı olduğunu göstermek amacıyla HTEA ve Hata Ağacı analizini entegre kullanmışlar ve hata modları ile güvenlik sistemleri yazılımları arasında güçlü bir ilişki olduğu sonucuna ulaşmışlardır. Schmittner v.d. (2014), klasik HTEA kapsamını güvenlik açıklıkları ve güvenliğe yönelik saldırıları kapsayacak şekilde genişleterek bir endüstriyel ölçüm sisteminde uygulamış ve modelin erken tasarım safhasında uygulanabilir bir model olduğu sonucuna varılmıştır. Silva v.d. (2016), büyük verinin kullanıldığı süreçlerde risk analizi yapmak amacıyla HTEA ve Gri teoriyi birlikte kullanmış ve sonuçta veri yönetiminin önemine dikkat çekmişlerdir.

Bowles ve Pelaez (1995), Hata Modu Etkileri Kritiklik Analizinde (FMECA) bulanık mantığa dayalı yeni bir yaklaşım sunmaktadır. Kullanılan bu yaklaşımda bulanık mantık sayesinde FMECA'da tanımlı arızalar önceliklendirilmekte ve mevcut veriler belirsiz olsa bile etkileri düzeltmeye ya da hafifletmeye yönelik eylemleri önceliklendirilmektedir. Xu v.d. (2002), bulanık olarak HTEA'nın değerlendirilmesini bir motor turboşarj sistemleri için gerçekleştirmişlerdir. Prototip değerlendirme uzman sistemi geliştirerek uzmanları HTEA sürecine tam olarak dahil etmiş ve ciddi oranda maliyet tasarrufu sağlamışlardır. Alizadeh v.d. (2022), HTEA ve bulanık HTEA yöntemlerini bir belediye atık su tesisindeki riskleri değerlendirmek ve önceliklendirmek için kullanmışlardır. Sonuçta; bu iki yöntem karşılaştırılmış ve bulanık HTEA'nın klasik HTEA'deki eksiklikleri azalttığı gözlenmiştir.

Silva v.d. (2014), BT sistemlerine bir saldırı olması durumunda potansiyel veri kayıplarını ve değişimlerini minimize etmek için HTEA ve bulanık teoriyi birlikte kullanmışlardır. Li v.d. (2018), bulanık ve gri HTEA kullanarak akıllı şehir sisteminde bilgi güvenliğinin beş boyutunu incelemişlerdir. Ershadi (2019), bilgi güvenliği risk yönetiminde HTEA ile MCDM yöntemlerinden AHP, TOPSIS ve Shannon Entropi yöntemleriyle karma bir yöntem kullanarak bilgi gizliliğinin en önemli bilgi güvenliği kriteri olduğu sonucuna varmıştır. Gusmão v.d. (2016), bilgi güvenliği risk analizi modelinde bulanık karar teorisini ve Olay Ağacı Analizini birlikte kullanmışlardır. Model daha sonra bir veri merkezinde test edilmiştir. Gusmão v.d. (2018), siber güvenlik risk analizi modeli çalışmasında Hata Ağacı Analizi ve bulanık karar teorisini kullanmışlardır.

Karabacak ve Soğukpınar (2005), bilgi güvenliğinde risk analizi için Bilgi Güvenliği Risk Analizi Yöntemini (ISRAM) önermişlerdir. Yöntem, bilgi güvenliği risklerini analiz etmek için nicel bir yaklaşım kullanmaktadır ve anket çalışması, risk tabloları ve basit matematiksel işlemler içermektedir. Shaikh ve Siponen (2023), bilgi güvenliğinde risk analizi çalışmasında üst yönetimin gösterdiği ilginin aracılık rolünü incelemişlerdir ve üst yönetim ile iş birliği yapılmasının oldukça önemli olduğu sonucuna varılmıştır. Ledermüller ve Clarke (2011) ise, mobil cihazlar üzerinde cihazların daha verimli çalışması amacıyla bir risk analizi çalışması yapmışlardır.

Edu v.d.(2021), finansal kurumların dijital dönüşüm süreçlerinde dijital uygulama ve platformların entegrasyonunda karşılaşılan güvenlik risklerini HTEA ve BTOPSİS yöntemlerini birlikte kullanarak analiz etmişler, en kritik güvenlik açıkları ve tehditler belirlemişlerdir. Ali v.d.(2022), çalışmalarında, Bangladeş bankacılık sektöründe BT sistemlerindeki başarısızlık faktörlerini HTEA ve TOPSIS kullanarak önceliklendirmişlerdir. Sonuçta ise siber saldırı, veri tabanı hack riskleri, sunucu arızası, ağ kesintisi, yayın veri hatası ve virüs etkisinin BT sisteminin başarısızlığı için en önemli faktörler olduğu sonucuna varılmıştır.

3. Bilgi Güvenliği

Bilgi güvenliği, bilgi varlıklarının her türlü riskten korunarak iş sürekliliğinin devamlılığını amaçlamaktadır (ISO, 2005). Bilgi güvenliğinde temel olarak üç unsur ele alınmaktadır: Gizlilik, Bütünlük ve Erişilebilirlik. Bu üç unsur, İngilizce karşılıklarının baş harfleri sebebiyle 'CIA üçlüsü' olarak bilinmektedir (Anderson, 2003; Dhillon ve Backhouse, 2000). Gizlilik, bilgiye yetkisiz erişimin önlenmesi ile ilgilidir. Bütünlük, yetkisiz kişilerce bilgi üzerinde değişiklik yapılmasını önlemek ya da en azından değişiklik yapılması durumunda değişikliği tespit etmekle ilgilidir. Erişilebilirlik ise bilgiye ne zaman istenirse o zaman erişebilmekle ilgilidir (Stamp, 2011). Bilgi güvenliğinde risk analizi ile BT kaynaklarına yönelik ihlallerin olması durumunda oluşacak zararları seviyelendirmek ve sıralamak amaçlanmaktadır (Shaikh ve Siponen, 2023). Bilgi güvenliğine yönelik risklerin analizinde birçok yöntem bulunmaktadır. Bu çalışmada, bankacılık sektöründe mobil cihazlara yönelik bilgi güvenliği riskleri bulanık HTEA yöntemi kullanılarak analiz edilmektedir.

4. HTEA

HTEA; kritik sistemlerde potansiyel hatanın olasılığını, şiddetini ve tespit edilebilirliğini değerlendirerek ürün/hizmet müşteriye ulaşmadan önce hataları belirlemek, analiz etmek ve hata etkilerini azaltmak amacıyla birçok sektörde kullanılmaktadır (Stamatis, 2003; Ivancan ve Lisjak, 2021; Carlson, 2012). Resmi olarak ilk kez 1960'ta NASA tarafından önerilmiş, daha iyi tanınırlığa ulaşması ise yaklaşık 1977 yılında Ford tarafından kullanılması ile olmuştur (Gilchrist, 1993; Sharma v.d., 2005). HTEA hataları önleyebilmekte ya da hataların etkisini azaltabilmekte, böylece müşteri memnuniyetiyle birlikte maliyet tasarrufu da sağlayabilmektedir (Carlson, 2012).

HTEA'da risk hesabı, risk öncelik sayısı (RÖS) kullanılarak yapılmaktadır. RÖS; hata modunun ortaya çıkmasının olasılığı (O), şiddeti (S) ve tespit edilebilirliğinin (D) çarpılması ile elde edilen bir değerdir (Mandal, 2014). RÖS hesaplamasında, başlangıçta elde edilen nitel bilgiler yorumlanarak nicel değerlere dönüştürülmektedir (Franceschini ve Galetto, 2001).

$$RPN=OxSxD \qquad (1)$$

RÖS; belirli bir değerin üzerinde olduğunda düzeltici eylem gerektirmektedir, bu değer Ghosh (2010) tarafından 80 üzeri olarak önerilmektedir. Düzeltici eylem uygulandıktan sonra daha düşük RÖS hedeflenmektedir.

Denklem (1)'de, olasılık, şiddet ve tespit edilebilirlik değerleri sıfırdan büyük ve bulanık olmayan sayılardır, dolayısıyla RÖS değerleri de bulanık olmayacaktır. Ancak klasik HTEA'daki bu yaklaşımın bazı dezavantajları bulunmaktadır (Mandal, 2014). HTEA; ürün ve süreçlerdeki yüksek kalite ve güvenilirlik sağlamakta, müşteri memnuniyetine katkıda bulunmaktadır. Ayrıca israfı önleyerek katma değeri olmayan süreçleri azaltmakta, maliyet tasarrufunu ve sürekli iyileştirmeyi desteklemektedir (Franceschini ve Galetto, 2001; Lipol ve Haq, 2011).

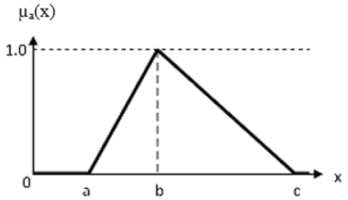
Ancak avantajlarına rağmen klasik HTEA'nın bazı dezavantajları da bulunmaktadır: RÖS değeri hesaplanırken elde edilen sonuç her zaman gerçekçi olmayabilir. Tüm parametrelerin eşit öneme sahip olması nedeniyle, farklı parametre değerlerinde aynı RÖS değerini veren hata modları için aynı yorumlamalar yapılacaktır. Örneğin; (O, S, D) endeksleri sırasıyla (8,8,1) olan bir hata modu ile (4,4,4) olan diğer bir hata modunun her ikisinde de RÖS değeri '64' olacaktır. Oysa ki O, S, D parametrelerinin değerleri de önemlidir. Ayrıca; parametrelerde bir değerin diğerinden daha iyi olduğu ya da daha kötü olduğu bilgisi dışında oransal olarak bilgi vermemektedir. Örneğin; '4' derecesi, '1' derecesinden dört kat daha kötüdür anlamına gelmemektedir. Sayısal veriler iyi yorumlama imkânı sağlarken zaman zaman analizin gerçekten uzaklaşma riskini de içermektedir. Bunun haricinde klasik HTEA dilsel değerlendirmelerin birleştirilmesi ve birden fazla hata modunun aynı zamanda meydana gelmesinin olasılık dağılımlarını hesaplamak oldukça zor olmaktadır. Bu dezavantajların giderilmesi için birçok yöntem kullanılmaktadır. Bulanık yaklaşım da bu yöntemlerden biridir.

5. Bulanık Mantık ve Bulanık HTEA

Gerçek dünya her zaman karmaşıklık içermekte ve karmaşıklığın giderilebilmesi için bireyler; kesin olan yerine yaklaşık olanı düşünerek tutarlı sonuçlar elde edebilme yeteneklerini kullanmaktadırlar. Bu noktada, yaklaşık olanı düşünme 'Bulanık Mantık' olarak karşımıza çıkmaktadır. Bulanık mantığın amacı; girdiler ile çıktıları birbirine mantık kuralları kullanılarak bağlamaktır (Chen ve Pham, 2000; Şen, 2020).

Bulanık mantıkta temel bileşenler; bulanıklaştırma, bulanık kural tabanı, bulanık çıkarım sistemi ve durulaştırmadır. Sırasıyla; modeldeki girdiler uygun dilsel ifadeler ile bulanıklaştırılmakta; girdi ve çıktı değişkenlerinin belirli değer aralıkları, kurallar çerçevesinde birbiriyle ilişkilendirilmektedir. Bulanık çıkarım sisteminde 'Eğer' ve 'ise' ler kullanılarak öncül ve ardıl ifadeler birbirleriyle eşleştirilmektedir. Son olarak da bulanık olarak elde edilen çıktı değişkeni durulaştırılarak net bir sayısal değer elde edilmektedir (Sharma, 2005; Şen, 2020).

Bulanık küme teorisi, belirsizlik içeren doğal dil kavramlarının farklı türde bulanık kümelerle ifade edilmesine ve esnek kullanılmasına olanak sağlamaktadır. Dilsel kavramlar, belirsiz olmakla birlikte anlamları ve yorumları bağlama göre değişmektedir. Bulanık kümeler ile analiz yapılırken çeşitli üyelik fonksiyonları kullanılmaktadır: Üçgen, yamuk ve sigmoid üyelik fonksiyonları en bilinenleridir. Çalışmada, dar bir değer aralığında (1-10) daha uyumlu geçişler sağladığı düşünüldüğü ve üyelik derecesinin 1'e eşit olduğu tek bir değer olması istenildiği için (öz değeri) üçgen üyelik fonksiyonu tercih edilmiştir. Bu kararın alınmasında karar vericilerin tercihleri göz önünde bulundurulmuş olup özün birden fazla değer alması istenildiğinde yamuk üyelik fonksiyonu da tercih edilebilmektedir. Ayrıca alt aralıklarda geçişler, birbirlerine tam teğet olmadığı için daha uzlaştırıcı bir çözüm sağlamaktadır (Jain, 2012; Şen, 2020).



Şekil 1: Üçgen Üyelik Fonksiyonu (Şen, 2020)

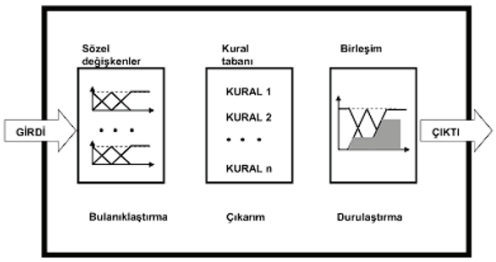
Üyelik fonksiyonu, $\mu_{A(x)}$ ile gösterilmektedir ve E evrensel kümesine ait bir *x* elemanının A alt kümesine ait olma derecesini ifade etmektedir. Fonksiyonda [0,1] sürekli aralığı kullanılmaktadır ve 0, *x* elemanının kümenin üyesi olmadığını göstermekte iken; 1, *x*'in kümenin tam üyesi olduğunu ve bu iki değer arasındaki herhangi bir sayı olan *x* ise kümeye ait olma derecesini ya da kısmi üyeliğini göstermektedir (Bojadziev ve Bojadziev, 1997; Maués v.d., 2019).

Bulanık A kümesinin Şekil 1'de gösterilen a, b ve c parametrelerine göre tanımlanmış üçgen üyelik fonksiyonunun matematiksel ifadesi:

$$\mu_A(\mathrm{x}) = \begin{cases} 0, & x < a \\ \frac{x-a}{b-a}, & a \le x \le b \\ \frac{c-x}{c-b}, & b \le x \le c \\ 0, & x > c \end{cases} \qquad (2)$$

5.1. Bulanık Çıkarım Sistemleri (BÇS)

Bulanık sistemlerin modellenmesinde Bulanık Çıkarım Sistemlerinden yararlanılabilmektedir. Literatürde Mamdani ve Tagaki-Sugeno Modeli en bilinenleri olmak üzere çeşitli Bulanık Çıkarım Sistemleri bulunmaktadır. Mamdani Modelinde öncüller ve ardılların tümü bulanıktır. Bulanık girdiler kural tabanı ile bulanık çıktılara bağlanmaktadır. Şekil 2'de Mamdani Modeli gösterilmektedir.



Şekil 2: Mamdani Modeli (Şen, 2020)

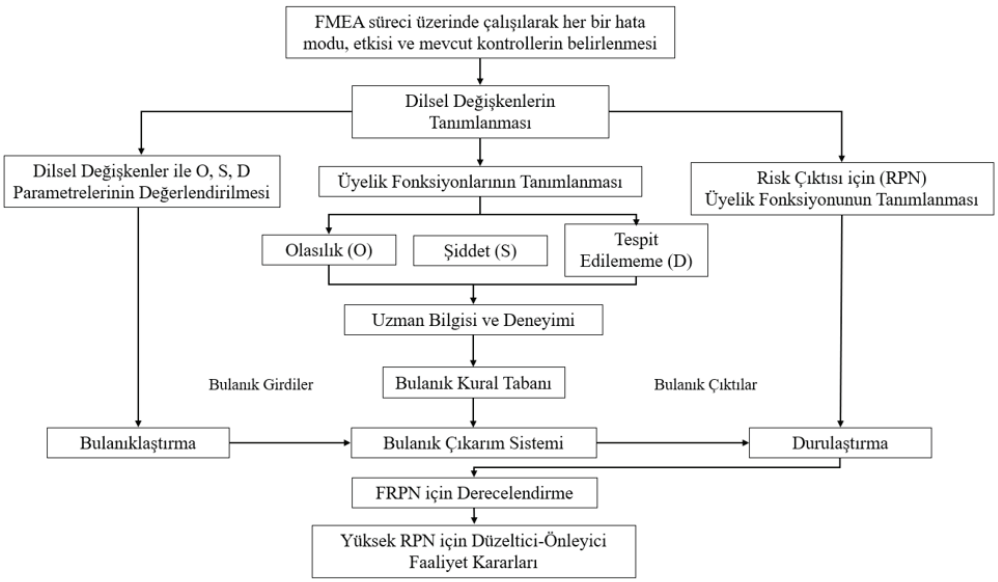
Bulanık çıkarım sistemlerinin işlem basamakları:

1. Bulanıklaştırma: Kural tabanında kullanılmak üzere girdi parametreleri, üyelik fonksiyonları aracılığıyla bulanıklaştırılır.
2. Çıkarım Yapılması: 've' mantıksal operatörü ile öncüldeki üyelik derecelerinin tamamı için en küçükleme ya da çarpım çıkarımı kullanılarak üyelik fonksiyonu eğrisinde istenilen aralık belirlenir ve ardıl için çıktı üretilir.
3. Kuralların Birleştirilmesi: 'veya' operatörü ile tüm kurallar için ortak bir çıkarım yapılarak bir önceki adımda belirlenen bulanık çıkarım fonksiyonları birleştirilerek en büyükleme yapılır. Bu adımda oluşan bulanık kümenin konveksliğinden ve normalliğinden söz edilememektedir.
4. Durulaştırma: Bulanıklaştırmanın tam zıttı olan durulaştırma işlemi, kuralların birleştirilmesi sonucunda elde edilen şekilden anlamlı bir nicel ifade elde edilmesidir. Sonuç değeri için genellikle eğri altındaki alanın ağırlık merkezi kullanılmaktadır. Ağırlık merkezi durulaştırma yöntemi için Formül (3) kulanılmaktadır (Buriboev v.d.,2019; Şen, 2020).

$$Z = \frac{\int \mu c(z) z dz}{\int \mu c(z) dz} \qquad (3)$$

5.2. Bulanık HTEA Prosesi

Bulanık HTEA, net bilgi içermeyen durumlarda girdi parametrelerini üyelik fonksiyonları yardımıyla bulanıklaştırarak kural tabanı yardımıyla klasik HTEA'nın dezavantajlarını gidermeye yönelik kullanılan bir tekniktir (Balaraju v.d., 2019). Bulanık HTEA süreç akış şeması Şekil 3'teki gibi özetlenebilir:



Şekil 3: Bulanık HTEA Prosesi (Chanamool v.d., 2016; Balaraju v.d., 2019)

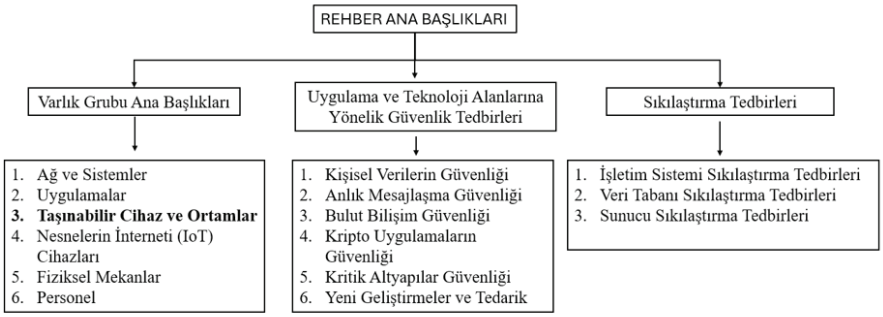
Bulanık HTEA sürecinde temel aşamalar aşağıdaki gibi sıralanabilir:

- Bulanık HTEA analizi yapılacak konu hakkında uzmanların önerileriyle hata modları ve potansiyel etkileri belirlenir.
- Girdi değişkenlerinin her biri için dilsel değişkenler tanımlanarak parametrelerin üyelik fonksiyonları belirlenir. Ek olarak bu aşamada RÖS değeri için de üyelik fonksiyonu belirlenir.
- Girdi değişkenlerinin tüm kombinasyonlarını içerecek şekilde üyelik fonksiyonları tanımlanır.
- Bulanık çıkarım sistemi ile durulaştırma işlemi yapılarak hesaplanan BRÖS değerleri önceliklendirilir.
- Son olarak da yüksek RÖS değerleri için düzeltici ya da önleyici faaliyetler önerilir (Chanamool v.d., 2016).

6. Uygulama

Kurumlarda, genel çerçevede bilgi varlıklarının güvenlik gereksinimlerini belirlemek, bilgi varlıklarının yönetimi ve belgelendirilmesini sağlamak amacıyla Uluslararası Standardizasyon Kuruluşu (ISO) tarafından ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı 2005 yılında yayınlanmış olup 2013 ve 2022 yıllarında standart değişen gereksinimlerle birlikte yenilenmiştir. Bu standardı detaylandırmak amacıyla da ISO/IEC 27002 standardı geliştirilmiştir (ISO/IEC 27002, 2005; ISO/IEC 27001, 2024). İlgili standartlarda varlık gruplarının ve kritiklik derecelerinin belirlenmesi, boşluk analizlerinin yapılması için yöntemlerin seçimi kurumlara bırakılmıştır. Bilgi güvenliğine yönelik çalışmalar yıllar içerisinde bu standartla sınırlı kalmayarak 2020 yılında ülkemizde de Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan Bilgi ve İletişim Güvenliği Rehberi yayımlanmıştır. Rehberde, ISO BGYS standardında detaylandırılmayan varlık gruplarına yönelik kritiklik dereceleri ve kritiklik derecelerine bağlı olarak alınması gereken tedbirler genel olarak belirlenmiştir ve bu tedbirlerin uygulanabilirliğinin denetimi için de 2021 yılında denetim rehberi yayımlanmıştır (Bilgi ve İletişim Güvenliği Rehberi, 2020; Bilgi ve İletişim Güvenliği Denetim Rehberi, 2021). Çalışma kapsamında, Bilgi ve İletişim Güvenliği Rehberinde yer alan Varlık Gruplarına Yönelik

Güvenlik Tedbirleri içerisinden 'Taşınabilir Cihaz ve Ortam Güvenliği' başlığı kullanılmıştır (Bilgi ve İletişim Güvenliği Rehberi, 2020). Rehber üç temel başlıktan oluşmaktadır. Şekil 4'te rehberde yer alan temel başlıklar ve alt grupları gösterilmektedir (Bilgi ve İletişim Güvenliği Rehberi, 2020).



Şekil 4: Bilgi Güvenliği Rehberi Ana Başlıkları (Bilgi ve İletişim Güvenliği Rehberi, 2020).

Çalışmada varlık gruplarına yönelik güvenlik tedbir maddelerinden yararlanılmıştır. Varlık grupları içerisinden Taşınabilir Cihaz ve Ortam Güvenliği alt başlığının seçilmesinde çalışanların tümünde veri ve sistemlere erişim için taşınabilir cihaz ve ortamların kullanılıyor olması, taşınabilir cihaz ve ortamlara bağımlı varlık gruplarının ve varlıkların sayısının ve kritikliğinin diğer varlık gruplarına göre yüksek olması etkili olmuştur. Gruptaki varlıkların sayıca fazla olması varlıkların güvenilirliklerinin kontrolünü de zorlamaktadır. Çalışma, kurumdaki ISO 27001 BGYS Ekip üyeleri ile yürütülmüştür. Üyeler, aynı zamanda CBDDO Bilgi Güvenliği Denetim Çalışmasını yürütmekte ve bilgi güvenliği alanında yetkin kişilerdir. Yedi kişilk bu ekip üyelerinin ünvanları ve tecrübe düzeyleri birbirlerinden farklı olup bu durum değişkenlerin yorumlanması konusunda çeşitlilik sağlamıştır.

Bankacılık sektöründe çalışmakta olan bilgi güvenliği uzmanlarının görüşlerinden ve daha önce yapılmış olan örnek diğer çalışmalardan yararlanılarak bu çalışmada Bulanık HTEA yöntemi kullanılmıştır. Hata modları belirlenirken Rehberde, Taşınabilir Cihaz ve Ortam Güvenliği Başlığında yer alan güvenlik tedbirleri incelenerek çalışma yapılan kurum için uygulanabilir olan 21 adet hata modu seçilmiştir. Çizelge 1'de belirlenen 21 hata modu listesi verilmektedir. Belirlenen hata modlarının O, S ve D değerlerinin yüksek olması güvenlik zafiyetlerinin yaşanma olasılığını artırmaktadır.

Çizelge 1. Hata Modları Listesi

	Hata Modları
1	Kurum verisine erişen taşınabilir bilgisayarlar için tanımlanmış kullanım politikası eksikliği.
2	Kurumun, mobil cihaz üzerinden e-posta ve/veya VPN gibi kurumsal servislere erişim izni vermeden önce politikayı çalışanlara tebliğ
3	Kritik veriye erişen cihazlara çeşitli yazılım kurulum kısıtlarının getirilmemesi.
4	Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgelerin kurumsal olarak yetkilendirilmemiş kişilerde veya kişisel olarak kullanılan cihazlarda bulundurulması.
5	Cihazı uzaktan fabrika ayarlarına döndürüp içindeki veriyi silebilecek bir mekanizmanın kullanılmaması.
6	Taşınabilir bilgisayarlar için gerekli güvenlik yazılımlarının yüklenmemesi.
7	Zararlı yazılımdan korunma uygulamalarına ait politikaların merkezi olarak yönetilmemesi.
8	Zararlı yazılımlardan korunma uygulamasının üretici veya ilgili kurum tarafından önerilen şekilde yapılandırılmaması ve güncel tutulmaması.
9	Tamire verilen taşınabilir bilgisayarlarda bulunan verinin silinmemesi.
10	Taşınabilir bilgisayarlar için çalınma ve kaybolma riskine karşı disk şifreleme yapılmaması.
11	Kritik veriye erişim imkânı olan taşınabilir bilgisayarlarda, harici depolama ortamlarının okuma ve yazma özelliklerinin devre dışı bırakılmış olmaması.
12	Kritik veriye erişen cihazların merkezi olarak yönetilmemesi. (Bu durum farklı kullanıcı grupları veya departmanlar arasında farklı güvenlik ayarlarına neden olabilir.)
13	Güvenlik politikasının kritik veriye erişen cihazlara yüklenmiş olmaması.
14	Merkezi yönetim sisteminin, güvenlik yamaları yüklenmemiş ya da üzerinde kara listeye alınmış uygulama/uygulama sürümü barındıran taşınabilir bilgisayarların sisteme erişiminin engellememesi.
15	Taşınabilir ortam yönetimine ilişkin en az fiziksel koruma ve saklama ile ilgili gereksinimler, yedekleme, el değiştirme ve imha hususlarını içeren kullanım politikası hazırlanıp uygulanmaması.
16	Taşınabilir ortamların, olumsuz fiziksel etkilere karşı üretici tarafından tavsiye edilen saklama ve kullanım koşullarına uyumlu olarak
17	Taşınabilir ortamlar üzerinde yer alan kritik bilginin/verinin şifreli olarak saklanmaması.
18	Kullanım süresi dolmuş taşınabilir ortamların veri sızıntılarını önlemek amacıyla güvenli olarak imha edilmemesi.
19	Taşınabilir ortam içindeki bilginin/verinin saklanması gereken süre göz önünde bulundurularak güvenli şekilde yedeklenmemesi.
20	Kritik seviyeli ağlarda kullanılan taşınabilir cihazların, internete bağlı veya kurum dışı sistemlerde kullanılması.
21	Kaba kuvvet saldırılarından korunmak için kurum tarafından belirlenecek sayıda hatalı giriş denemesi sonrası cihaz belleğinde bulunan verilerin silinmemesi.

Çalışmada ilk adımda klasik RÖS hesaplaması yapılmış sonra ise bulanık RÖS hesaplaması yapılarak bu iki sonuç karşılaştırmalı olarak değerlendirilmiştir. RÖS değeri için karar vericilere 'Çok Düşük', 'Düşük', 'Orta', 'Yüksek' ve 'Çok Yüksek' olmak üzere 5'li ölçek sunulmuştur.

Çalışmada, Matlab paket programı (Versiyon: MatlabR2024a) içerisindeki Bulanık Mantık (Fuzzy Logic) Modülü kullanılmıştır. Kullanılan Bulanık HTEA temelde;

- Girdi olarak olasılık, şiddet ve tespit edilememe olmak üzere üç parametreden,
- Girdi parametrelerini üyelik dereceleriyle birlikte dönüştüren bulanıklaştırma ara yüzünden,
- Tüm kombinasyonları içerecek şekilde çok sayıda Eğer-İse kuralını içeren kural tabanından,
- Bulanık sonuçlar içeren çıktı ara yüzünden oluşmaktadır.

Çalışmada girdilerin ve çıktıların bulanık sayılar olduğu durumlarda kullanılan Mamdani Bulanık Çıkarım Sistemi kullanılırken bulanık çıkarım aşamasında, girdiler arasından en küçük üyelik derecesine sahip değerin belirleyici olması istenildiği için EK-EB metodu kullanılmıştır. Durulaştırma için ise en çok tercih edilen yöntem olan ağırlık merkezi metodu uygulanmıştır. Kesin değerlerin bulanık değerlere dönüştürüldüğü girdi arayüzünde üyelik fonksiyonlarının tipi ile parametre değerleri belirlenmektedir. Çalışmada, en yaygın kullanımlardan biri olan üçgen üyelik fonksiyonu seçilmiştir. Alt aralıklardaki geçiş değerlerinin birbirine tam olarak teğet olmaması nedeniyle, üyelik fonksiyonundaki geçişler daha uzlaştırıcı bir çözüm sunmaktadır. Dilsel değişkenler yardımıyla parametrelerin her biri için bulanık aralıklar belirlenmelidir. Bunun için de mevcut ölçeklendirme kılavuzları incelenerek 10'lu dilsel ölçekte değerlendirme yapılmasına karar verilmiştir. Risk puanlaması yapılırken kullanılan açıklamalar için yine literatür örnekleri incelenerek Chanamool v.d. (2016) çalışmasında uygulandığı gibi dilsel değişkenler; 1=Çok Düşük (ÇD), 2-3= Düşük (D), 4-6= Orta (O), 7-8= Yüksek (Y) ve 9-10= Çok Yüksek (ÇY) olmak üzere 5 seviyede ele alınmıştır. Bulanık kuralların belirlenmesi adımında tüm kombinasyonlar için kural yazılacağından 5 seviyede gruplanan dilsel değişkenler için 5^3=125 adet kural tanımlanmıştır. Tüm karar vericilerden alınan değerler, medyan değeri hesaplanarak birleştirilmiştir.

Girdilere ait üyelik fonksiyonları:

$$\mu(O,S,D)_{\text{ÇD}} = \begin{cases} \frac{x+2}{2}, & -2 \le x \le 0 \\ \frac{2-x}{2}, & 0 \le x \le 2 \\ 0, & x < -2; x > 2 \end{cases} \quad (4)$$

$$\mu(O,S,D)_{\text{D}} = \begin{cases} \frac{x-1}{1,5}, & 1 \le x \le 2,5 \\ \frac{4-x}{1,5}, & 2,5 \le x \le 4 \\ 0, & x < 1; x > 4 \end{cases} \quad (5)$$

$$\mu(O,S,D)_{\text{O}} = \begin{cases} \frac{x-3}{2}, & 3 \le x \le 5 \\ \frac{7-x}{2}, & 5 \le x \le 7 \\ 0, & x < 3; x > 7 \end{cases} \quad (6)$$

$$\mu(O,S,D)_{\text{Y}} = \begin{cases} \frac{x-6}{1,5}, & 6 \le x \le 7,5 \\ \frac{9-x}{1,5}, & 7,5 \le x \le 9 \\ 0, & x < 6; x > 9 \end{cases} \quad (7)$$

$$\mu(O,S,D)_{\text{ÇY}} = \begin{cases} \frac{x-8}{2}, & 8 \le x \le 10 \\ \frac{12-x}{2}, & 10 \le x \le 12 \\ 0, & x < 8; x > 12 \end{cases} \quad (8)$$

Bu değerler Matlab bulanık mantık ara yüzünde tanımlanmıştır. Girdilere ait parametreler ve değer aralıkları, üyelik fonksiyonu tipi vb. belirlendikten sonra çıktı fonksiyonuna ait değerler girilmiştir. Çalışmada, 5'li ölçek ile değerlendirme yapılmıştır.

Bulanık aralıklar girdi parametrelerinde olduğu gibi Çok Düşük(ÇD), Düşük(D), Orta(O), Yüksek(Y) ve Çok Yüksek (ÇY) olarak kategorilere ayrılmıştır. Risk aralıkları, RÖS değerindeki yığılmaları göz önüne alarak belirlenmiş olup RÖS değerleri öncesinde klasik bir risk analizi çalışması için yaklaşık risk puanı sınırları Çizelge 2'deki gibi belirlenmiştir:

Çizelge 2. RÖS İçin Belirlenen Değer Aralıkları ve Hata Modu Frekans Değerleri

Klasik HTEA için RÖS Değer Aralıkları							
Alt Sınır				**Üst Sınır**	**Tanım**	**Kısaltma**	**Frekans**
10	<=	RÖS Değeri	<	18	Çok Düşük	ÇD	4
18	<=	RÖS Değeri	<	40	Düşük	D	7
40	<=	RÖS Değeri	<	84	Orta	O	5
84	<=	RÖS Değeri	<	126	Yüksek	Y	3
126	<=	RÖS Değeri	<	200	Çok Yüksek	ÇY	2

Çizelge 2'de yer alan alt ve üst sınır değerleri aynı zamanda hesaplananan RÖS değerleridir. Sınır değerlerinin bir alt ve bir üst sınırlara dâhil edilmesini kolaylaştırmak için böyle bir yol izlenmiştir. Bu sayede örneğin, 84 RÖS değeri hem 'O' hem de 'Y' risk seviyesine üye olacaktır.

Çıktı için üçgen üyelik fonksiyonları:

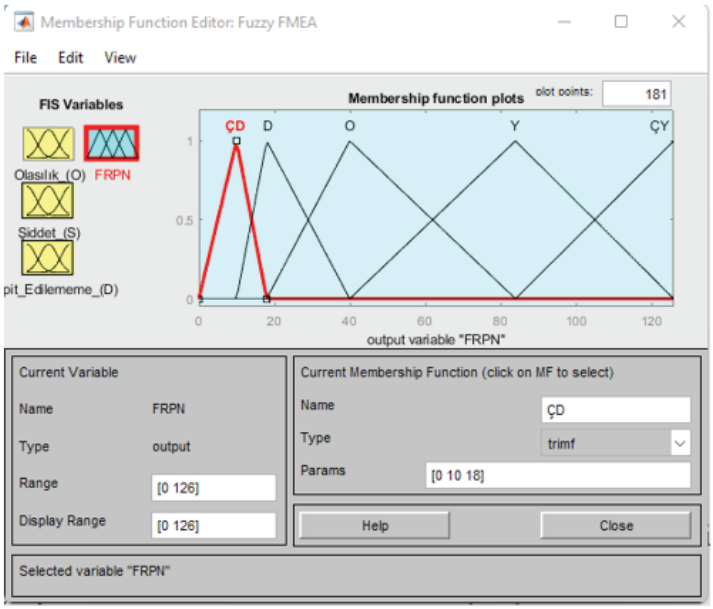
$$\mu(O,S,D)_{ÇD} = \begin{cases} \frac{x}{10}, & 0 \le x \le 10 \\ \frac{18-x}{8}, & 10 \le x \le 18 \\ 0, & x < 0; x > 18 \end{cases} \quad (9)$$

$$\mu(O,S,D)_{D} = \begin{cases} \frac{x-10}{8}, & 10 \le x \le 18 \\ \frac{40-x}{22}, & 18 \le x \le 40 \\ 0, & x < 10; x > 40 \end{cases} \quad (10)$$

$$\mu(O,S,D)_{O} = \begin{cases} \frac{x-18}{22}, & 18 \le x \le 40 \\ \frac{84-x}{44}, & 40 \le x \le 84 \\ 0, & x < 0; x > 18 \end{cases} \quad (11)$$

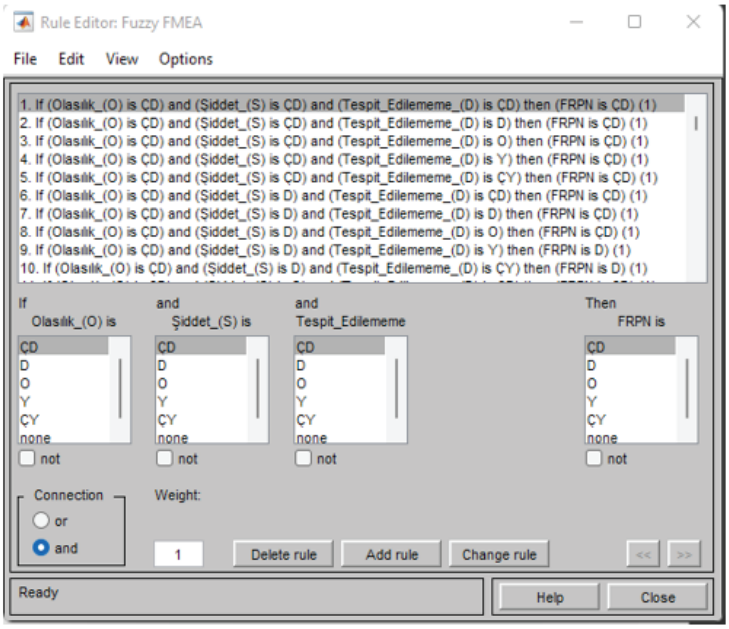
$$\mu(O,S,D)_{Y} = \begin{cases} \frac{x-40}{44}, & 40 \le x \le 84 \\ \frac{126-x}{42}, & 84 \le x \le 126 \\ 0, & x < 40; x > 126 \end{cases} \quad (12)$$

$$\mu(O,S,D)_{ÇY} = \begin{cases} \frac{x-84}{42}, & 84 \le x \le 126 \\ \frac{200-x}{74}, & 126 \le x \le 200 \\ 0, & x < 84; x > 200 \end{cases} \quad (13)$$

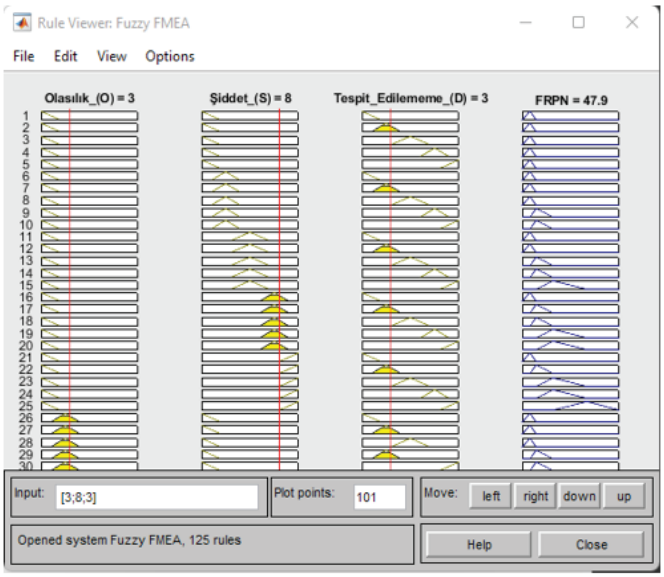


Şekil 5: Çıktı Değişkenine Ait Üyelik Fonksiyonu

Matlab programında çıktı değişkenine ait parametrelerin tanımlanmasıyla Şekil 5'teki gibi simetrik olmayan üçgen üyelik fonksiyonları ortaya çıkmıştır. Kural tabanının oluşturulma aşamasında birçok Eğer-İse kuralı belirlenebilmektedir. Çalışmada 125 adet bulanık kural belirlenmiştir. En uygun olan kuralların bulunması, modelin başarısını artırmada kritik bir unsurdur. Şekil 6'da örnek olarak ilk 10 kural gösterilmektedir.



Şekil 6: Oluşturulan Kural Tabanı



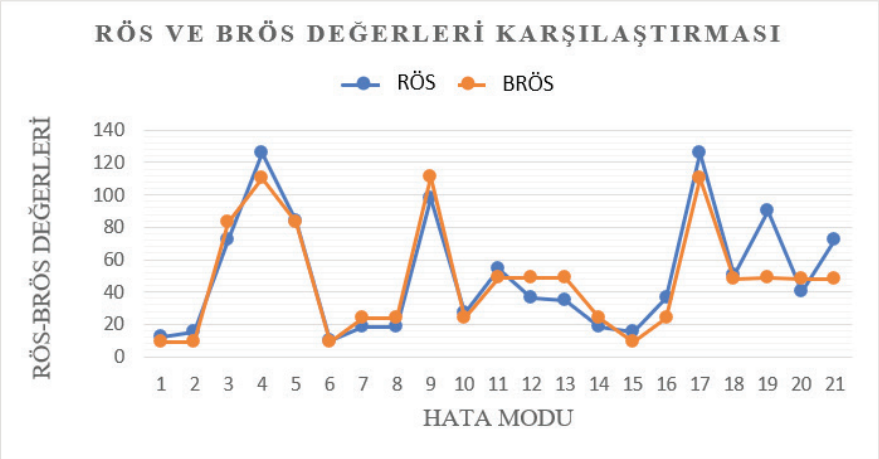
Şekil 7: Kural Görüntüleyici Ara Yüzü- Hata modu 21 için BRÖS değeri.

Şekil 7'de 21 numaralı hata modu için girdi değerleri (3,8,3) ve BRÖS değerinin 47,9 olarak hesaplandığı görülmektedir. Benzer şekilde tüm hata modları için BRÖS değerleri hesaplanmıştır. Hesaplanan RÖS ve BRÖS değerleri Çizelge 3'te gösterilmektedir.

Çizelge 3. Anket Sonucunda Hesaplanan RÖS ve BRÖS değerleri

Hata Modu No	MEDYAN			RÖS	BRÖS
	O	S	D		
1	1	4	3	12	9,24
2	1	5	3	15	9,24
3	2	9	4	72	83,20
4	2	9	7	126	110,00
5	3	7	4	84	83,20
6	1	10	1	10	9,24
7	1	9	2	18	23,50
8	2	9	1	18	23,50
9	2	7	7	98	111,00
10	1	9	3	27	23,50
11	2	9	3	54	48,60
12	2	9	2	36	48,60
13	1	10	4	35	48,60
14	1	9	2	18	23,50
15	1	6	3	15	9,24
16	2	6	3	36	23,50
17	2	9	7	126	110,00
18	2	5	5	50	47,90
19	3	6	5	90	48,60
20	2	10	2	40	47,90
21	3	8	3	72	47,90

Çalışmanın sonunda hesaplanan RÖS ve BRÖS değerleri, Şekil 8'deki gibi grafiksel olarak karşılaştırılmıştır.



Şekil 8: RÖS ve BRÖS Değerleri Karşılaştırması

7. Sonuç

Teknolojinin sürekli olarak gelişmesi beraberinde birçok yeni tehdit unsurları ve zafiyet ortaya çıkarmaktadır. Dolayısı ile bilgi güvenliğine yönelik sayılamayacak kadar çok risk mevcuttur ve yeni teknolojiyle birlikte riskler de sürekli yenilenmektedir. Bilgi varlıklarının korunması bireylerin ve kurumların güvenilirliği ve devamlılığı için oldukça önemlidir. Bilgi güvenliğinin sağlanması için de riskler iyi belirlenmeli, önceliklendirilmeli ve önlemler alınmalıdır. Ayrıca bu işlem dinamik hale getirilmeli, sürdürülebilir olmalı ve gelişen teknolojiye ve değişen tehditlere toleranslı olmalıdır.

Bu çalışma, bankacılık sektöründe taşınabilir cihaz ve ortam güvenliğinin önemli risklerini belirleme ve değerlendirme amacını taşımaktadır. Risk analizi yöntemleri içerisinde sıklıkla tercih edilen bulanık HTEA yöntemi kullanılmıştır. Belirsiz durumlar için daha esnek çözüm sunduğu için klasik HTEA yöntemi yerine bulanık HTEA yöntemi tercih edilmiştir. Bilgi güvenliği alanında 7 uzman, 21 hata modunu 10 farklı dilsel ölçekte değerlendirmiştir. Uzmanların farklı disiplinlerden gelmesi ve tecrübe düzeylerinin farklılığı ile özellikle belirli hata modlarının farklı yorumlanması sonucunu ortaya çıkarmıştır. Değerlendirmeler sonucunda aykırı puanların yer almaması için her girdi için medyan değeri esas alınarak çalışma gerçekleştirilmiştir.

Ayrıca klasik RÖS hesaplaması ile bulanık RÖS sonuçları bir grafik yardımıyla karşılaştırılmış ve beklendiği üzere iki değerin birbiriyle oldukça tutarlı olduğu sonucuna varılmıştır. İki yöntem arasındaki korelasyon katsayısı da hesaplanmış olup bu değer 0,924 seviyesindedir. Çıkan değer, bulanık HTEA'nın geleneksel yöntemle güçlü bir uyum içinde olduğunu göstermektedir. Bulanık HTEA'da farklı olarak üyelik derecesi 1 olmayan değerler kesin olarak bir gruba üye olmak yerine iki gruba kısmi üye oldukları için daha esnek sonuç sunmaktadır.

Çalışma sonucunda hata modları bulanık Risk Öncelik Puanlarına göre sıralandığında, yüksek öncelik verilmesi gereken 5 hata modu;

1. Tamire verilen taşınabilir bilgisayarlarda bulunan verinin silinmemesi,
2. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgelerin kurumsal olarak yetkilendirilmemiş kişilerde veya kişisel olarak kullanılan cihazlarda bulundurulması
3. Taşınabilir ortamlar üzerinde yer alan kritik bilginin/verinin şifreli olarak saklanmaması,
4. Kritik veriye erişen cihazlara çeşitli yazılım kurulum kısıtlarının getirilmemesi,
5. Cihazı uzaktan fabrika ayarlarına döndürüp içindeki veriyi silebilecek bir mekanizmanın kullanılmaması, olarak belirlenmiştir.

Kritik önemli risklerin ve kabul edilebilir risk kategorisi düzeyine inmesi için etkili önlemlerin alınması gerekmektedir. Örneğin; Taşınabilir bilgisayarların tamire verilmesi durumunda içerisindeki verilerin mutlaka silinmesi gerekmektedir. Taşınabilir ortamda yer alan veriler ilgili politika ve prosedürlerde bahsi geçtiği şekilde ve belirtildiği süre boyunca saklanmalıdır. Politikalar ve prosedürler belirli aralıklarla gözden geçirilmeli ve gerektiğinde güncellenmelidir. Düzenli olarak güvenlik denetimleri yapılmalı, güvenli yazılım ve donanımlar kullanılmalıdır. Ayrıca personele yönelik farkındalık eğitimleri düzenlenmeli, organizasyonlarda bilgi güvenliği kültürü oluşturulmalıdır. Önlemlerin alınmaması halinde ise gizli bilgilerin yetkisiz kullanıcıların eline geçmesi ve kötü amaçlarla kullanılması, finansal kayıplar, itibar kaybı, hukuki maliyetler gibi bir dizi olumsuz durumların ortaya çıkma ihtimali bulunmaktadır.

Bankacılık sektöründe taşınabilir cihaz ve ortamların bilgi güvenliği risklerini ele alarak, bu alanda çalışan uzmanlar ile birlikte sektöre özel bir risk analizi çalışması yapılmıştır. Analizde kullanılan Bulanık HTEA yöntemi ile belirsizliklerin daha etkin yönetilmesi ve önceliklendirilmesi sağlanmıştır. Bu yaklaşım, bankaların taşınabilir cihaz ve ortamların bilgi güvenliği risklerinin belirlenmesine ve önceliklendirilmesine katkı sağlamaktadır. Risklerin dikkate alınması halinde müşteri bilgilerini koruma, finansal kayıpları önleme ve sektördeki güvenilirliği artırma açısından kritik bir rol oynamaktadır. Ayrıca, çalışma taşınabilir cihaz güvenliği alanında referans sunarak gelecekteki araştırmalar için de bir rehber olması amaçlanmıştır. Çalışma kapsamı taşınabilir ortam ve cihaz güvenliği ile sınırlandırılsa da gelecekte, rehberde yer alan diğer varlık grupları üzerinde de risk analizi çalışması yapılarak kurumların risk önceliklendirilmesine katkı sağlanabilir. Ayrıca varlık grupları haricinde kalan diğer ana başlıklar için de çalışma tekrarlanabilir. Risk analizlerinin kapsamının genişletilmesi ile daha çok hata modu incelenebilir ve böylece daha gerçekçi bir risk değerlendirilmesi yapılabilir.

Kaynakça

1. Ali, S. M., Hoq, S. N., Bari, A. M., Kabir, G., and Paul, S. K. (2022). Evaluating factors contributing to the failure of information system in the banking industry. Plos one, 17(3), e0265674.
2. Alizadeh, S. S., Solimanzadeh, Y., Mousavi, S., and Safari, G. H., (2022). Risk assessment of physical unit operations of wastewater treatment plant using fuzzy HTEA method: a case study in the northwest of Iran. Environmental Monitoring and Assessment, 194(9), 609.
3. Anderson, J. M., (2003). Why we need a new definition of information security. Computers & security, 22(4) 308-313.
4. Balaraju, J., Raj, M. G., and Murthy, C. S., (2019). Fuzzy-HTEA risk evaluation approach for LHD machine–A case study. Journal of Sustainable Mining, 18(4) 257-268.
5. Bidgoli, H., (2006). Handbook of information security, information warfare, social, legal, and international issues and security foundations, Vol. 2, John Wiley & Sons,.
6. Bojadziev, G., and Bojadziev, M., (1997). Fuzzy logic for business, finance, and management Vol. 12, World Scientific.
7. Bowles, J. B., and Peláez, C. E., (1995). Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis. Reliability engineering & system safety, 50(2) 203-213.
8. Buriboev, A., Kang, H. K., Ko, M. C., Oh, R., Abduvaitov, A., and Jeon, H. S., (2019). Application of fuzzy logic for problems of evaluating states of a computing System, 9(15) 3021.
9. Carlson, C. S., (2012). Effective HTEAs: Achieving safe, reliable, and economical products and processes using failure mode and effects analysis, Vol. 1, John Wiley & Sons,
10. Chanamool, N., and Naenna, T., (2016). Fuzzy HTEA application to improve decision-making process in an emergency Department, 43 441-453.
11. Chen, G., and Pham, T. T., (2000). Introduction to fuzzy sets, fuzzy logic, and fuzzy control systems, CRC press, Boca Raton,
12. Chiozza, M. L., and Ponzetti, C., (2009). HTEA: a model for reducing medical errors. Clinica chimica acta, 404(1) 75-78.
13. de Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Poleto, T., and Costa, A. P. C. S., (2016). Information security risk analysis model using fuzzy decision theory. International Journal of Information Management, 36(1) 25-34.
14. de Gusmão, A. P. H., Silva, M. M., Poleto, T., e Silva, L. C., and Costa, A. P. C. S., (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory, 43 248-260.
15. Dhillon, G., and Backhouse, J., (1996). Risks in the use of information technology within organizations, 16(1) 65-74.

16. Edu, A. S., Agoyi, M., & Agozie, D. (2021). Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis. PeerJ Computer Science, 7, e658.
17. Ershadi, M. J., and Forouzandeh, M., (2019). Information Security Risk Management of Research Information Systems: A hybrid approach of Fuzzy HTEA, AHP, TOPSIS and Shannon Entropy. J. Digit. Inf. Manag., 17(6) 321.
18. Franceschini, F., and Galetto, M., (2001). New approach for evaluation of risk priorities of failure modes in HTEA. International journal of production research, 39(13) A 2991-3002.
19. Gilchrist, W., (1993).Modelling failure modes and effects analysis. International Journal of Quality & Reliability Management, 10(5)
20. Ghosh, M. (2010): 2017."Process failure mode effects analysis (PHTEA)." Retrieved January 5
21. International Standards Organization (ISO) (2005). ISO/IEC 17799 information technology security techniques: code of practice for information security management. Geneva: ISO;
22. ISO, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, www.iso.org/standard/27001 (Erişim tarihi: 1 Ekim2024)
23. Ivančan, J., and Lisjak, D. (2021). New HTEA risks ranking approach utilizing four fuzzy logic systems. Machines, 9(11) 292.
24. Jain, M. K., (2012). An Efficient Expert System Generator for Qualitative Feed-Back Loop Analysis. BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 3(1) 5-18.
25. Karabacak, B., and Sogukpinar, I., (2005). ISRAM: information security risk analysis method. Computers & Security, 24(2) 147-159.
26. Kim, M.H., Toyib, W., and Park, M.G., (2013). An Integrative method of FTA and HTEA for software security analysis of a smart phone. KIPS Transactions on Computer and Communication Systems 2(12) 541-552.
27. Ledermüller, T., and Clarke, N. L., (2011). Risk assessment for mobile devices. Trust, Privacy and Security in Digital Business: 8th International Conference, TrustBus 2011, Toulouse, France, August 29-September 2, 2011, Proceedings 8. Springer Berlin Heidelberg,
28. Li, X., Li, H., Sun, B., and Wang, F., (2018). Assessing information security risk for an evolving smart city based on fuzzy and grey HTEA. Journal of Intelligent & Fuzzy Systems, 34(4) 2491-2501.
29. Lipol, L. S., and Haq, J., (2011). Risk analysis method: HTEA/FMECA in the organizations. International Journal of Basic & Applied Sciences, 11(5) 74-82.

30. Mandal, S., and Maiti, J., (2014). Risk analysis using HTEA: Fuzzy similarity value and possibility theory based approach. Expert Systems with Applications, 41(7) 3527-3537.
31. Maués, L. M. F., Sá, J. A. S. D., Costa, C. T. D., Kern, A. P., and Duarte, A. A. A. M., (2019). Construction duration predictive model based on factorial analysis and fuzzy logic. Ambiente Construído, 19 115-133.
32. Schmittner, C., Gruber, T., Puschner, P., and Schoitsch, E., (2014). Security application of failure mode and effect analysis (HTEA). In Computer Safety, Reliability, and Security: 33rd International Conference, SAFECOMP 2014, September 10-12, 2014. Proceedings 33 Springer International Publishing, Florence, Italy, p. 310-325.
33. Shaikh, F. A., and Siponen, M., (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security, 124 102974.
34. Sharma, R. K., Kumar, D., and Kumar, P., (2005). Systematic failure mode effect analysis (HTEA) using fuzzy linguistic modelling. International journal of quality & reliability management, 22(9) 986-1004.
35. Silva, M. M., de Gusmão, A. P. H., Poleto, T., e Silva, L. C., and Costa, A. P. C. S., (2014). A multidimensional approach to information security risk management using HTEA and fuzzy theory. International Journal of Information Management, 34(6) 733-740.
36. Stamatis, D. H., (2003). Failure mode and effect analysis, Quality Press
37. Stamp, M., (2011). Information security: principles and practice, John Wiley & Sons
38. Şen, Z. (2020). Bulanık mantık ilkeleri ve modelleme. Su Vakfı.
39. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Denetim Rehberi 2020,https://cbddo.gov.tr/SharedFolderServer/Projeler/File/BG_Denetim_Rehberi.pdf (Erişim tarihi: 1 Ekim 2024).
40. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi 2021, https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf (Erişim tarihi: 1 Ekim 2024).
41. Xu, K., Tang, L. C., Xie, M., Ho, S. L., & Zhu, M. L. (2002). Fuzzy assessment of HTEA for engine systems. Reliability engineering & system safety, 75(1), 17-29.
42. Yang, Z., Bonsall,S., and Wang, J.. (2008). Fuzzy rule-based Bayesian reasoning approach for prioritization of failures in HTEA. IEEE Transactions on Reliability 57.3 517-528