SİBER SALDIRILARIN TESPİTİ ve ENGELLENMESİ İÇİN UZMAN SİSTEM (US) TASARIMI: SİBER SAVUNMA UZMAN SİSTEMİ (SİSU)

Kerim Göztepe[*] Semra Boran[*] Harun Reşit Yazgan[*]

[*]Sakarya Üniversitesi Mühendislik Fakültesi, Endüstri Mühendisliği, Esentepe Kampüsü, 54187, Sakarya, Türkiye Tel: +90 264 295-5454

kerimgoztepe@gmail.com
boran@sakarya.edu.tr
yazgan@sakarya.edu.tr

Özet:

Günümüzde bilişim teknolojileri hızla gelişmekte ve hayatımızdaki birçok konu gibi kamunun tüm birimleri her geçen gün daha fazla teknolojiye bağımlı olmaktadır. Bilişim teknolojileri toplumun ihtiyaç duyduğu haberleşme, ulaşım (kara, hava, deniz), e-devlet, nüfus, vergi, savunma hizmetleri gibi birçok konuda büyük kolaylıklar sağlamaktadır. Ancak kötü niyetli eller teknolojik sistemleri birer silaha dönüştürebilir. Bu çalışmada Ulaştırma Denizcilik ve Haberleşme Bakanlığının (UDHB) bilişim sistemlerine yönelik yapılacak siber saldırıları tespit ve engellemek amacıyla bir uzman sistem (genel çerçevesi) tasarlanmıştır. Uzman sistemin kullanılması sayesinde UDHB bilişim uzmanlarının herhangi bir siber saldırıyı anlama ve karşı koymak için gerekli tedbirleri alma süresi kısalacaktır.

Anahtar Kelimeler: Siber saldırılar, uzman sistemler, Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB)

1. Giriş

Uzman sistemler 1960'larda Nobel Fizyoloji ve Tıp Ödülü sahibi Joshua Lederberg'in spektrograf verilerinin bilgisayarlı yorumları üzerine yaptığı çalışmalarla ortaya çıkmaya başlamıştır[1],[2]. Birçok araştırmacının ilgisini çeken uzman sistemler, yapay zekânın problem çözme alanının dışına çıkarak yeni bir kavram oluşturmuştur. Uzman sistemlerin kökeni geleneksel veri işlemedir. Araştırmacıların insanın sahip olduğu bilgi işleme yeteneğinin makine tarafından otomatik olarak gerçekleştirilmesi amacıyla yaptıkları çalışmalar[3] sonucunda uzman sistemler ortaya çıkmıştır.

Uzman Sistemler (US), belirli konuda uzman olan bir ve birçok insanın yapabildiği muhakeme ve karar verme işlemlerini modelleyen bir yazılım sistemidir. Bu programlar, sisteme girilen belirli bir probleme hızlı ve seri bir şekilde çözümler getiren, sistem tasarımına bağlı olarak sorunları gidermek için bir iş dizisi öneren programlardır [4]. Bir uzman sistemin sahip olduğu en önemli özelliği, büyük bir bilgi tabanına sahip olmasıdır. Buradaki kritik husus; değişme ve gelişmeye açık olması gereken bilgi tabanı bölümüyle statik olması gereken program bölümünün birbirinden ayrılmasıdır[5].

Uzman Sistemler hakkında birçok bilim adamı tarafından farklı tanımlar yapılmıştır. İngiliz Bilgisayar Birliği Uzman Sistem Grubu'nun yapmış olduğu tanıma göre; uzman sistem, uzman bir kişinin becerilerinden oluşan bilgiyle donatılmış bir bilgisayarın içinde akıllıca önerilerde bulunan veya bir işlev hakkında kararlar verebilen sistem yapısıdır[6]. Harmon ve King "Uzman sistemler öneri geliştirme, analiz yapma, iletişim kurma, danışmanlık yapma, teşhis etme, tasarım yapma, açıklama yapma, öngörüde bulunma, buluş yapma, öğrenme, yönetme, anlatma, öğretme ve planlama yapma amaçlarıyla kullanılabilir"[7] tanımını yapmıştır.

Uzman sistemler tıp, mühendislik, hukuk gibi birçok alanda kullanılmaktadır. Çeşitli bilim dalları uzman sistemlerine ait örnekler Tablo 1'de verilmiştir.

Tablo 1. Uzman sistem örnekleri [8].

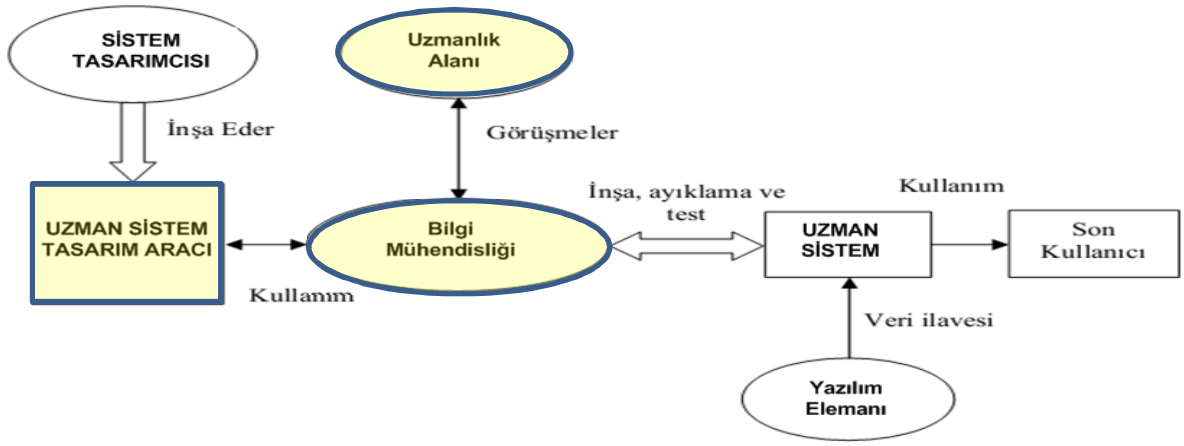
ACES	Haritalarda kartografik işlemlerin yürütülmesi.
MYCIN	Bakteriyel enfeksiyonların teşhis ve tedavisi.
ADEPT	Muharebede taktik önerilerin verilmesi.
AIRID	Uçağın türünün görsel bilgilere göre belirlenmesi.
AIRPLAN	Uçak gemilerinde uçakların kalkış, ve inişinin yönlendirilmesi.
DART	Keşif bilgilerinin değerlendirilmesi.

CADUCEUS	Dâhili hastalıkların teşhisi.
HASP	Muharebelerin nerelerde olabileceğinin tahmini.
ONCOCIN	Kemoterapi hastalarının tedavi ve idaresi.
ACE	Telefon ağlarındaki arızaların teşhisi.
IN-ATE	Osiloskop hatalarının teşhisi.
NDS	Ulusal iletişim ağının teşhisi.
LITHO	Petrol kuyularının verilerinin yorumlanması.

2. Uzman Sistemlerin Genel Yapısı

Uzman Sistemler (US), belirli bir alanda ihtiyaç duyulan ancak o konunun uzmanı tarafından cevaplanabilen problemleri çözebilmekte ve elde edilen sonuçları belli bir formatta saklayabilmektedir. Bu nedenle US'ler bilgiye dayalı sistemler (knowledge based systems) olarak adlandırılmaktadır.

Bir uzman sistemini oluşturan üç ana unsur vardır. Bunlar uzmanlık alanı, bilgi mühendisliği ve uzman sistem tasarım aracı olarak tanımlanabilir (Şekil 1).



Şekil 1. Bir uzman sistemin yapısı [5].

Uzman sistemlerin insan altyapısını oluşturan uzman personel, bilgi mühendisi ve kullanıcı tanımları aşağıda verilmiştir.

2.1. Uzman Personel

Uzman personel, kendi uzmanlık alanında bilgi seviyesi yüksek, konusuyla ilgili problemlere özel çözümler üretmek için bilgisine başvurulan kişidir. Uzman kişi ilgi alanında mevcut sorunlara daha etkin çözüm için araştırmalar yapmakta, özgün ve pratik teknikler ortaya koymaktadır. Uzman kişi aynı zamanda probleme ait çözümleri modelleyebilmeli ve bu modelleri uzman sistem oluşturmada kullanabilmelidir[9].

2.2. Bilgi Mühendisi

Bilgi mühendisi, genellikle yapay zekâ konusunda bilgi sahibi kişidir ve uzman sistemlerin nasıl yapılacağını bilir. Bilgi mühendisi uzmanlarla görüşerek bilgiyi organize ederek, bu bilgilerin bir uzman sistem içerisinde nasıl temsil edileceğine karar verir. Ayrıca, yazılım hazırlamak ve düzenlemek için programcılara yardım eder[9].

Uzman sistem tasarım aracı bilgisayar programlama yazılımlarından farklıdır. Uzman sistem tasarımında kullanılacak yazılım aslında bir yapay zekâ programlama dili veya uzman sistem geliştirme kabuğudur. Bu tür yazılımlar bilgi mühendisi veya uzman sistem programlayıcı tarafından uzman sistem tasarımında kullanılmaktadır.

2.3. Kullanıcı

Kullanıcı, tasarlanan uzman sistemi kullanan kişidir. Kullanıcı bilim adamı, teknisyen veya tasarlanan uzman sistem hakkında eğitim almış birisi olabilir. Buchanan'ın tasarladığı kural tabanlı uzman sistemin uzmanlardan

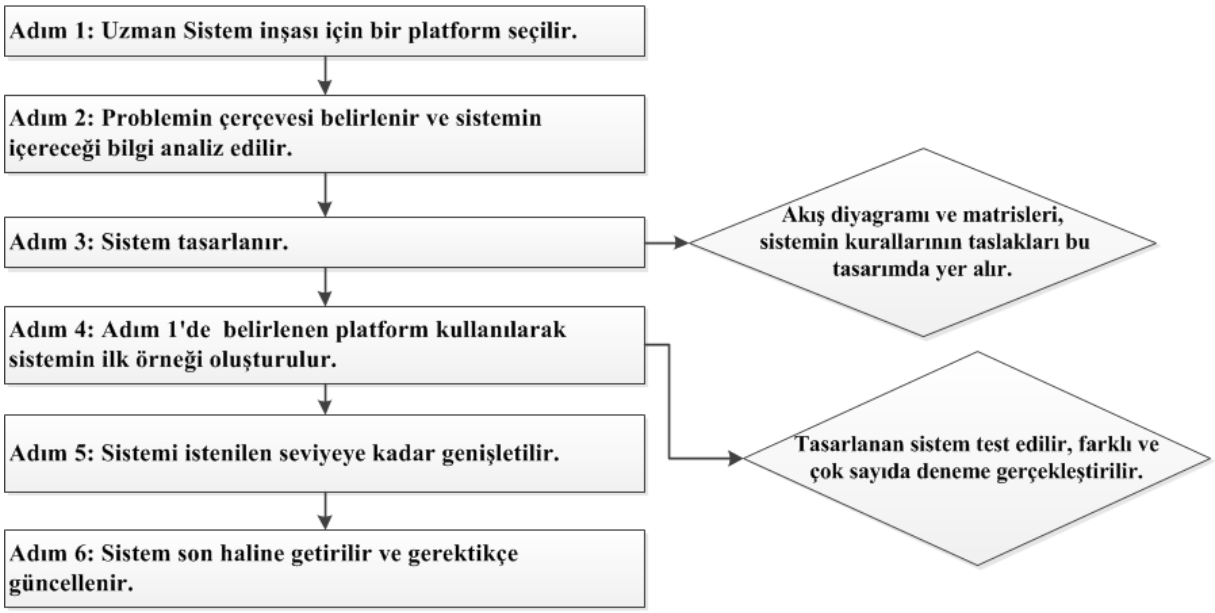
daha doğru ve hızlı karar verdiği anlaşıldıktan sonra uzman sistemlerin kullanıcı yelpazesi oldukça genişlemiştir[10].

3. Uzman Sistemlerin Tasarım Aşamaları

Uzman sistem tasarımcılarının bu sistemleri geliştirmede göz önünde bulundurdukları bazı esaslar vardır. Bunlar;

a. İhtiyaç duyulan bir yerde mevcut olmayan bir uzmanın yerini alabilmesi,
b. Konusuna hâkim birçok uzmanın bilgi ve tecrübe birikimini aynı programda toplaması,
c. Sistemi kullanacak uzmanları veya sistemin ait olduğu bilim dalındaki uzman adaylarını eğitebilmesi, uzmanları ilgilendirmeyen veya uzmanların pahalı olduğu projeler için gerekli uzmanlığı sağlamak olarak sıralanabilir.

Uzman sistemin tasarımında aşağıdaki adımlar uygulanır (Şekil 2).



Şekil 2. Uzman sistem tasarımı.

Bir uzman sistem problemi değerlendirip karar verme yeteneğine sahiptir. Uzman sistem sahip olduğu verileri işleyerek istenenen sonucu veya istenen sonuca en yakın değeri belirler. Sistemin karar verme şekli bilgi tabanındaki bütün kuralların genellikle iki farklı yöntemle muhakeme edilmesiyle gerçekleştirilmektedir. Bu yöntemler[11]; ileriye doğru zincirleme ve geriye doğru zincirleme'dir.

3.1. İleriye Doğru Zincirleme

İleriye doğru zincirleme (forward chaining)'nin karar verme ünitesi, ***if-then*** kuralı esasına göre çalışmaktadır. Kural ***if*** ifadesinden başlar ***then*** kısmına ulaşmasıyla gerçekleşmiş olur. Bu kuralın "tümevarım" metoduyla çalışan mekanizması Şekil 3'de verilmiştir. Sistemde tanımlanan tüm kurallar gereken şartı sağlayarak sonuca ulaşmaktadır. Eğer gereklilik ifadesi ***if*** sağlanıyorsa, o zaman ***then*** kısmındaki yargı kısmı doğrulanmaktadır. Kuralın ifade ettiği şartlar yerine getiriliyorsa sonuç cümlesi sağlanmış olmaktadır[12].

Şekil 3. İleriye doğru zincirleme kuralı.

3.2. Geriye Doğru Zincirleme

Geriye doğru zincirleme (backward chaining)'nin karar verme ünitesi; kuralın en son ifadesi ***then*** ifadesi ile başlamakta ve şart ifadesi olan ***if*** ifadesiyle bitmektedir. Bu kuraldaki zincirleme sistemi "tümdengelim" metoduna göre çalışmaktadır. Kural ***then*** ifadelerini tek tek inceleyerek çalışmaktadır (Şekil 4).

Şekil 4. Geriye doğru zincirleme kuralı.

4. Uzman Sistemlerin Çalışma Prensibi

Uzman sistem kullanıcısı US programına gerçek durumu vermekte ve karşılığında uzman tavsiyesi veya uzmanlık almaktadır. Bu sistemler çoğunlukla iki ana unsura sahiptir. Bunlardan birincisi bilgi tabanı (knowledge base) olup, doğruluğu önceden bilinen gerçekleri içermektedir. Çalışmada örnek bilgi tabanı olarak Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UDHB) sistemlerinin (haberleşme, karayolları, demiryolları, havacılık, denizcilik) bağlı olduğu altyapı kabul edilmiştir.

İkinci unsur olan karar motoru (inference engine) ise, bilgi tabanı'nda bulunan bilgiyi kullanarak kullanıcının sorularına uygun sonuçları çıkarmaktadır[13]. Çalışmada tasarlanan SİSU'nun çalışma prensibi Şekil 5'te gösterilmiştir.

Şekil 5. SİSU çalışma prensibi

4.1. Araştırma Metodolojisi

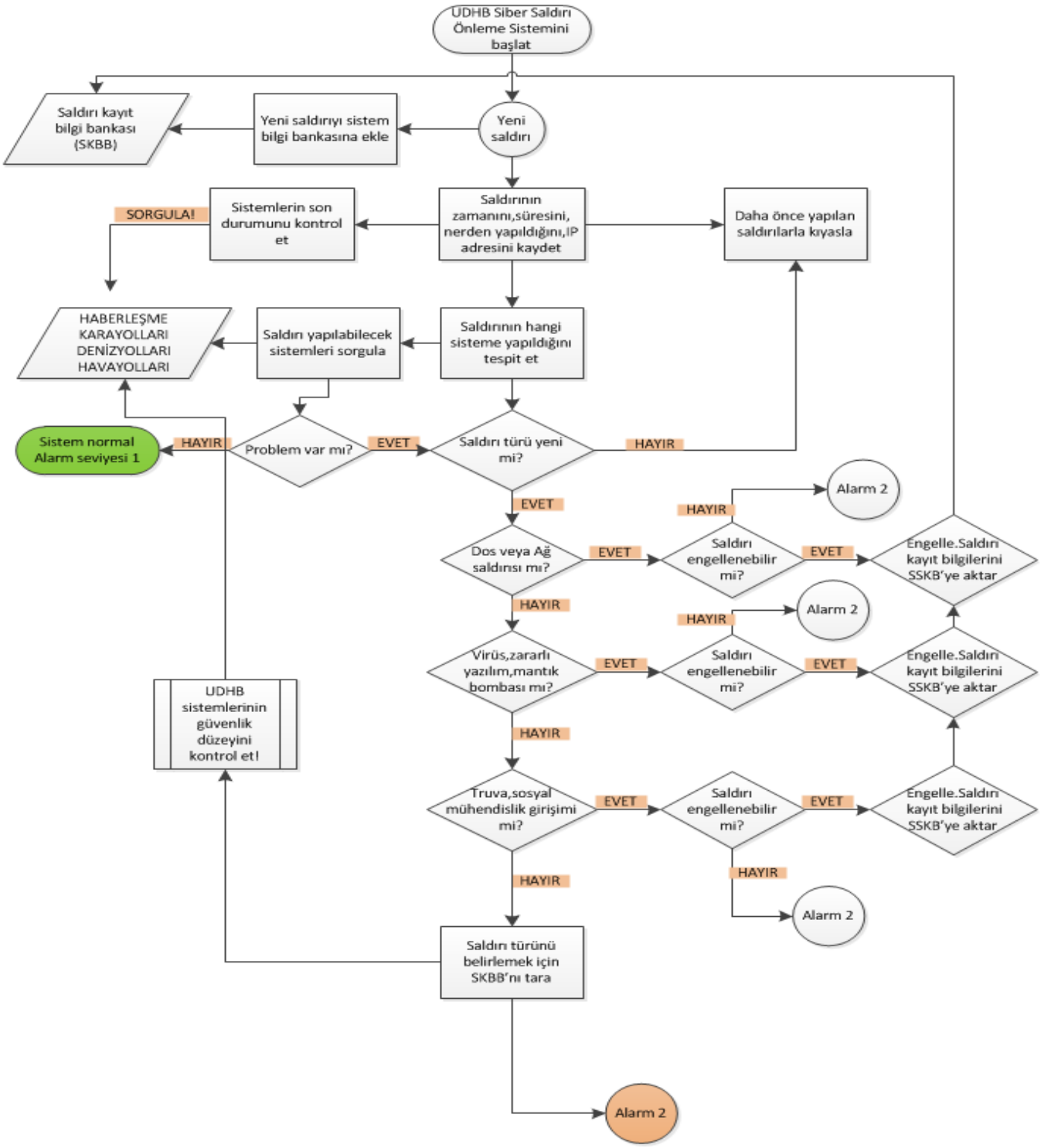
SİSU projesi; sistemi oluşturacak kriterlerin tanımlanması, sistemi kullanacak uzman personel, saldırı kayıt bilgi bankası (SKBB), UDHB sistemleri bilgi bankasının oluşturulması ile tasarım adımlarlardan oluşmaktadır.

Kriterlerin tanımlanması: SİSU projesini oluşturacak kriterler bu adımda belirlenir. SİSU projesi; sistemi kullananan personel, kullanıcı ara yüzü, saldırı kayıt bilgi bankası (SKBB), UDHB bağlı olduğu veri bankası ve SİSU kriterlerinden oluşmuştur.

SİSU Uzman Personeli: SİSU kullanıcısı, sistemin çalışma prosedürünü çok iyi bilen uzman personel veya bu konuda eğitim almış personelden seçilir. Personel UDHB sistemleri ve özelliklerine hâkim olmalıdır. Uzman personel aynı zamanda tespit ettiği sistem açıklarını giderebilmelidir.

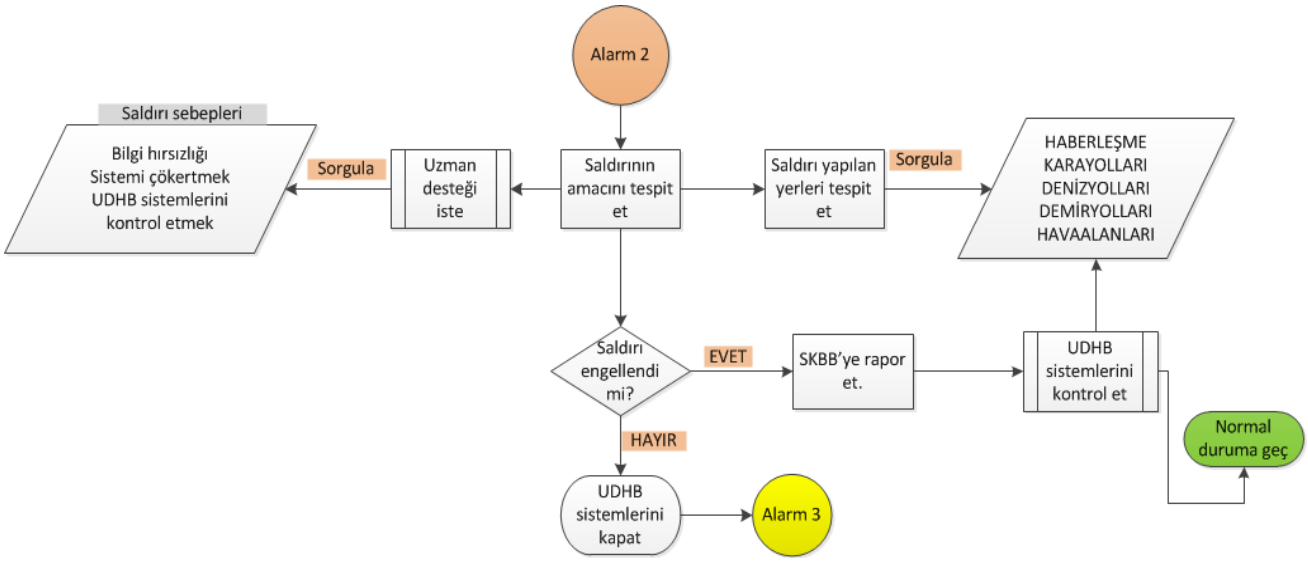
SKBB ve UDHB Sistemleri Bigi Bankası: SİSU projesinde SKBB ve UDHB sistemleri olmak üzere iki ana bilgi bankası tasarlanmıştır. UDHB sistemleriyle ilgili tüm teknik detaylar UDHB Sistemleri Bilgi Bankası'nda yer almalıdır (UDHBSBB). UDHBSBB' de bakanlığın sorumlu olduğu sistemlere ait detaylı tüm bilgiler olmalıdır.

Tasarım: SİSU sisteminin ilk adımı sistemin başlatılmasıdır. Sistem başladıktan sonra, kullanıcı personel herhangi bir siber saldırı anında kullanıcı arayüzü sayesinde müdahele etmek istediği konuyla ilgili bilgi alabilecektir. SİSU sisteminin çalışma prensipleri ve tasarımı Şekil 6,7 ve 8'de verilmiştir. SİSU başlatıldıktan sonra sisteme yeni bir saldırı olup olmadığına bakar. Saldırı mevcutsa saldırının zamanını, tespit edilirse yeri, IP adresi vb. bilgileri kaydeder. Diğer adımlarla ilgili bilgiler Şekil 6'da ifade edilmiştir.



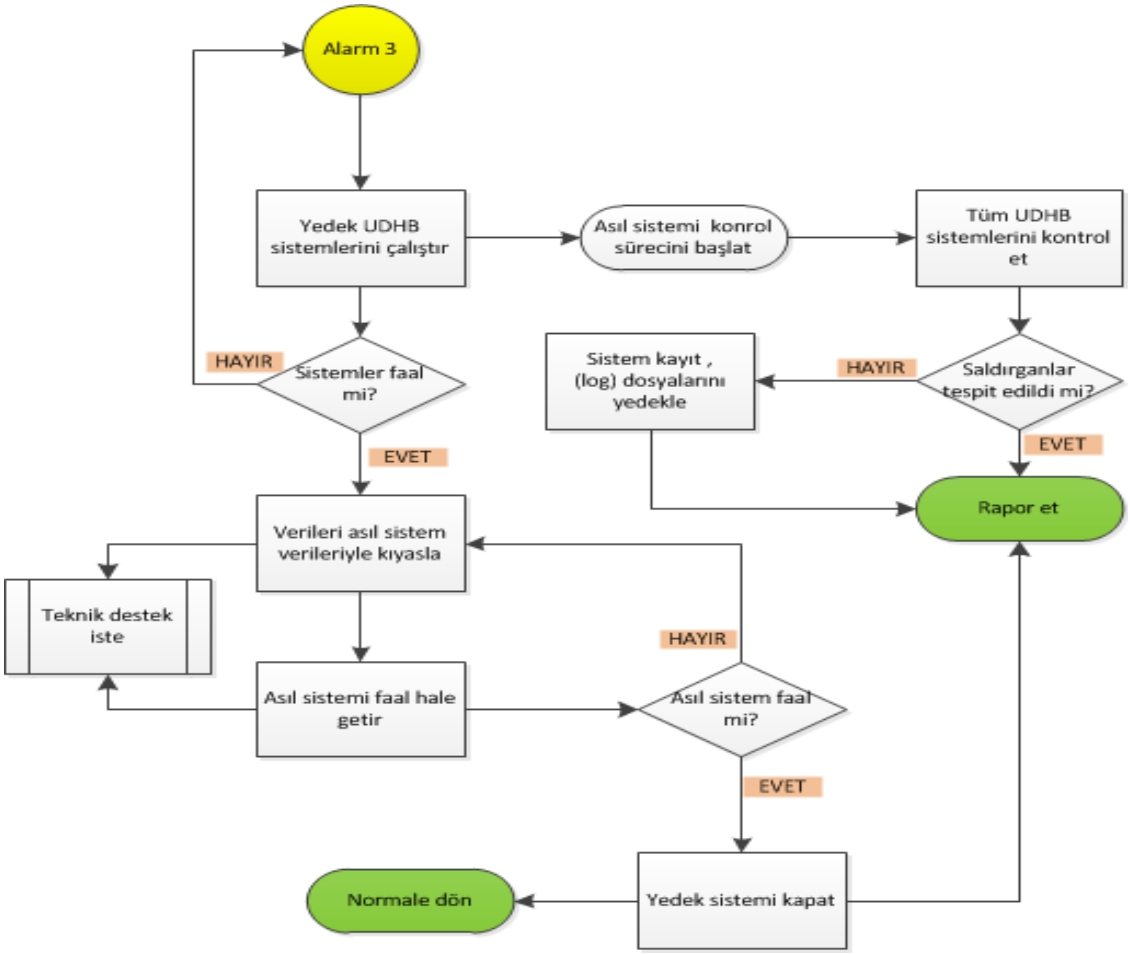
Şekil 6. Sistemin başlatılması

SİSU saldırıyı tespit edemez veya engelleyemez ise Alarm 2 moduna geçilir. Alarm 2 modunda uzman desteği istenmelidir. Teknik ekip ve cihaz desteğiyle UDHB sistemlerinin son durumları kontrol edilmeli, vakit kaybetmeden sistem sorgulanmalıdır. Saldırıyı engelleme başarısız olursa Alarm 3 moduna geçilmelidir.



Şekil 7. Alarm 2 modülü.

Alarm 3 modunda yedek sistem başlatılır. Yedek sistem sayesinde UDHB sistemleri faal tutulurken asıl sistem kontrol edilmelidir. Bu işleme saldırıların tepit edilip asıl sistemin faaliyete geçirilmesine kadar devam edilir. Yapılan tüm işlemler kayıt edilmelidir. Asıl sistem çalışmaya başladıktan sonra yedek sistem devreden çıkarılır.



Şekil 7. Alarm 3 modülü.

4.2. Tasarlanan SİSU Sisteminin Beklenen Faydaları

SİSU genelde şu özellikleri taşıyacak şekilde tasarlanmıştır.

Hızlı Cevap Verme: SİSU, sorulan sorulara bir uzmandan daha hızlı ve makul sürede cevap verebilmelidir. Bu sayede siber saldırılara karşı reaksiyon süresi kısalacaktır.

Yüksek Performans: SİSU, istenen bilgileri bir uzman kadar veya ondan daha iyi düzeyde verebilmelidir. Sistemden alınan bilgiler beklentileri karşılamalıdır.

Anlaşılabilirlik: SİSU, elde ettiği sonucun aşamalarını açıklayabilmelidir. Sonuca nasıl vardığı bilinmeyen bir sistem akıllarda soru işareti bırakacaktır. Bu nedenle SİSU ulaştığı sonuçları istatiksel verilerle detaylandırmalıdır.

Güvenilirlik: SİSU, güvenilir olmalı ve hata vermemelidir. Yapılacak hatalar bir siber saldırı anında yanlış tedbirlerin alınmasına neden olabilir.

5. SONUÇ

Günlük hayatımızı kolaylaştıran onlarca uygulama, bilgi, doküman internet ortamında rahatça bulunabilmektedir. Ancak bu durum kötü niyetli kullanıcılar ve dolandırıcılar, gizli belgelere ulaşmak isteyen özel eğitimli kişiler, siber aktivistler gibi internet ortamının sunduğu sınırsızlıktan yararlanmak isteyen kişilere fırsatlar sunmaktadır. İnternetin yaygın olarak kullanılmaya başlanmasıyla birlikte başta sağlık, eğitim, finans olmak üzere tüm kamu kurumları ve özel sektör yoğun olarak bilişim teknolojilerini bünyelerine entegre etmiştir. Bu kurum ve kuruluşlara ait sistemlere yapılacak bir siber saldırı günlük hayatı felç edecektir[14]. Bu kuruluşlardan belkide en önemlisi internet hizmetlerinin omurgasını teşkil eden UDHB'dir. Bu nedenle siber saldırılara karşı güçlü bir işletim sistemiyle birlikte [15] siber uzman sistemlerin kullanılması önemli bir konu olarak ortaya çıkmıştır.

Bu çalışmada, UDHB sistemlerine yapılacak siber saldırılara daha etkin müdahele etmek maksadıyla bilgi tabanlı bir uzman sistemin genel çerçevesinin oluşturulması samaçlanmıştır. Konusuna hâkim uzman personellerin yardımıyla UDHB sistemlerine yapılacak saldırıların tespiti, kayıtlarının tutulması, sistem arızalarının bulunması, amaçlarıyla taslak bir uzman sistem, SİSU, tasarlanmıştır. Sistemin bilgi tabanı oluşturulurken UDHB sistemleri konusunda yetkili personelin bilgi ve tecrübesine başvurulması planlanmıştır. Tasarlanan uzman sistemde SKBB ve UDHBSBB olmak üzere iki bilgi bankası yer alacaktır. Sistem sayesinde siber saldırılara karşı daha hızlı ve etkin kararlar alınacağı değerlendirilmektedir.

6. Kaynaklar

[1] Lederberg, J., Lederberg, E. M., Zinder, N. D., Lively, E. R., "Recombination analysis of bacterial heredity", Cold Spring Harbor Symposia on Quantitative Biology 16:413-443, 1951.

[2] Morse, M. L., Lederberg, E. M., Lederberg, J., Sept. "Transductional heterogenotes in Escherichia coli", Genetics 41(5):758-779, 1956.

[3] Alty, I.; Coombs, M.J.: "Expert Systems: Concepts and Examples", Manchester NCC Publishing, England,1984.

[4] Wiig, K. M., Knowledge Management, The Central Management Focus for Intelligent-Acting Organization. Arlington: Schema Press, 1994.

[5] Waterman, D.,"A Guide of Expert Systems", Addison-Wesley Publishing Company, Massachusetts, USA, 1986.

[6] Vickry, A.; Brooks, H.: "Expert Systems and Their Applications in LISP", Online Review, 149-165, 1987.

[7] Harmon, P.; King, D.: "Expert Systems", Newyork, USA, 1985.

[8] Nabiyev, V., Yapay Zeka, Seçkin, Ankara, 2005.

[9] Koçyiğit, N., Merkezi Klima Sistemlerinde Arıza Giderme ve İşletim İçin Bilgi Tabanlı Uzman Sistem Geliştirilmesi, Marmara Üniversitesi, Fen Bilimleri Enstitüsü Doktora Tezi, İstanbul, 2008.

[10] Buchanan, B. G. and Shortliffe, E. H. Rule-based Expert systems: the MYCIN Experiment of the Stanford Heuristic Programming Project. Reading: Addison-Wesley, 1984.

[11] Derbyshire, I. L., "Development of EXCAPP, An Intelligent Knowledge Based Process Planning System For Turned Components" PhD Thesis, UMIST, 1985

[12] Edmund, C., Robert, C., Developing Expert Systems, J. Wiley Inc.,1990.

[13] Turban, E.: “Expert systems and applied artificial intelligence”, Macmillan publishing company, New York USA, 1992.
[14] Göztepe, K., “Designing a Fuzzy Rule Based Expert System for Cyber Security”, International Journal of Information Security Science, 1(1): 13-19, 2012.
[15] Göztepe, K., Ejder, A., “Operating System Evaluation Using Choquet Integral in Terms of Cyber Threats”, 5th International Conference on Information Security and Cryptology Proceedings, 50-54, 2012.