Araştırma Makalesi

Bankacılıkta Siber Güvenlik Üzerine Bibliyometrik Analiz

Ömer Faruk KORKMAZ[1], Selin SOĞUKOĞLU KORKMAZ[2]

[1] Öğr. Gör. Dr., Giresun Üniversitesi, Tirebolu Mehmet Bayrak MYO, omer.faruk.korkmaz@giresun.edu.tr, ORCID: 0000-0002-3283-6174
[2] Öğr. Gör. Dr., Giresun Üniversitesi, Keşap MYO, selin.korkmaz@giresun.edu.tr, ORCID: 0000-0001-9944-8494

Öz: Finansal teknolojinin bankacılık sektöründeki en son yansıması dijital bankacılıktır. Dijital bankacılık ile birlikte finansal güvenlik konusunda çeşitli endişeler ortaya çıkmaktadır. Gerçekleştirilen bu çalışma bankacılık sektöründe artan dijital kullanımın bir sonucu olarak ortaya çıkan siber güvenlik ihtiyacı ile ilgili yapılan literatür çalışmalarını konu edinmektedir. Bu çalışma ile bankacılık sektöründe siber güvenlik kullanımını ele alan literatürün sistematik değerlendirilmesi amaçlanmaktadır. Bu kapsamda Web of Science veri tabanında "banking" ve "cyber security" kavramları kullanılarak arama yapılmıştır. Sadece araştırma makaleleri tercih edilmiş ve bu bağlamda veri seti 88 çalışmadan oluşmuştur. Bu verilerin analizlerinde ve ilişki ağlarının görselleştirilmesinde Bibliometrix ve VOSviewer uygulamalarından yararlanılmıştır. İncelenen çalışmalarda yazarlara, anahtar kelimelere, atıf alma durumlarına, ülkelere, kaynakçalara göre öne çıkan ve etki düzeyi yüksek olan çalışma konularına yönelik analizler yapılmıştır. Çalışmada sonuç olarak 2019 yılı sonrası yayın sayılarının arttığı ve anahtar kelimeler bazında fintek ve siber güvenlik kavramlarına ilişkin kelimelerin daha çok ele alındığı tespit edilmiştir. Yayınların ülkelere göre dağılımı incelendiğinde konuyla ilgili en fazla yayın yapan ülkeler sırasıyla Hindistan, Pakistan, Ürdün, ABD ve İngiltere olmuştur. Güvenliğin riske verilen bir cevap olduğu bilinmektedir. Dolayısıyla siber güvenlik konusu proaktif bir şekilde ele alınmalıdır. Dahası düzenleyici ve denetleyici otoriteler, siber güvenlik şirketleri ve finansal sektör kuruluşları ileri teknoloji kullanımının yanı sıra çalışan kabiliyetlerini ve ekosistemlerini siber ihlallere karşı iyileştirmelidirler. Finansal kuruluşların zamanla dijital ayak izlerini genişleteceği bilinciyle siber güvenlik adına bugünden çevreyi hazır halde tutmak önem arz edecektir.

Anahtar Kelimeler: Siber Güvenlik, Dijital Bankacılık, Bibliyometrik Analiz
Jel Kodları: G210, G200, G290

A Bibliometric Analysis on Cyber Security in Banking

Abstract: The most recent reflection of financial technology in the banking sector is digital banking. With digital banking, various concerns about financial security arise. This study focuses on the literature on the need for cybersecurity, which has emerged due to the increasing digital usage in the banking sector. This study aims to systematically evaluate the literature on the use of cyber security in the banking sector. In this context, the Web of Science database was searched using "banking" and "cyber security". Only research articles were preferred; in this context, the data set consisted of 88 studies. Bibliometrix and VOSviewer applications were used to analyze these data and visualize the relationship networks. In the analyzed studies, analyses were made for the prominent and high-impact study topics according to authors, keywords, citation status, countries, and bibliographies. The study revealed increased publications after 2019, with a greater focus on keywords related to fintech and cyber security concepts. Upon analyzing the distribution of publications by countries, we found that India, Pakistan, Jordan, the USA, and the UK had the highest number of publications on the subject. Therefore, cyber security should be addressed proactively. Moreover, regulatory and supervisory authorities, cybersecurity companies, and financial sector institutions should improve their employee capabilities and ecosystems against cyber breaches and the use of advanced technology. Recognizing that financial institutions will expand their digital footprint over time, keeping the environment ready for cybersecurity today will be necessary.

Keywords: Cybersecurity, Digital Banking, Bibliometric Analysis
Jel Codes: G210, G200, G290

Atıf: Korkmaz, Ö. F. & Soğukoğlu Kormaz, S. (2025). Bankacılıkta siber güvenlik üzerine bibliyometrik analiz. *Fiscaoeconomia*, *9*(2), 1112-1127. https://doi.org/10.25295/fsecon.1595122

Geliş Tarihi: 02.12.2024
Kabul Tarihi: 10.02.2025

1. Giriş

Sanayi toplumundan bilgi toplumuna evirilmiş olan günümüz dünyası, edinilen bilginin görünür yansımaları olan teknolojinin ve inovasyonun etkilerine maruz kalmaktadır. Dünün dünyasında arazilerin büyüklüğü veya fabrikaların sayısı önem arz ederken bugünün dünyasında bilginin depolanması, işlenmesi ve aktarılması gibi unsurların fark yarattığı görülmektedir. Dolayısıyla artan rekabette öne çıkabilmek ve bu avantajı koruyabilmek için işletmelerin bilgi teknolojilerini yoğun bir şekilde kullandıkları, bu süreçte ise sektörlerin dijitalleştiği görülmektedir. Hemen hemen bütün sektörlerde işlemler elektronik ortamlarda yürütülmekte, muhasebe ve raporlamadan, alışveriş, ödeme ve transfer sistemlerine kadar birçok alanda yenilikler olmakta, internet tabanlı yazılım ve elektronik sistemlerin kullanımı artmaktadır. Elde edilen hız ve kolaylık kazanımlarıyla süreçlerde ve maliyetlerde iyileşme, operasyonel etkinlik ve verimlilik ile hizmet kalitesinde artma gibi faydalar sağlanmaktadır (Korkmaz vd., 2023). Ancak bilgi teknolojilerindeki bu yaygın kullanımının sunduğu fırsat ve faydaların beraberinde, tehditler ve riskleri de barındırdığı açıktır (Harvey & Lau, 2009). Bu tehdit ve risklerin en ciddi olanı ise siber saldırılardır. Bu saldırılar sonucu kurumlar ciddi maliyetlerle karşılaşmakta ve itibar kayıpları yaşamaktadırlar. Siber saldırılardan korunmak için kuruluşların gerekli tedbir ve önlemleri alarak bütün süreçlerini hazırlıklı tutmaları gerekmektedir. Bunun için ihtiyaç duyulan altyapıyı sağlamak, risk ve kontrol süreçlerini değerlendirmek, siber güvenlik denetimlerini çok iyi bir şekilde uygulamak önem arz etmektedir. Teknolojik gelişmeler ve artan yaygın kullanımı ile birlikte dijitalleşen işlem ve ilişkilerin çokluğu mahremiyet, gizlilik, güvenlik gibi konuların gelecekte çokça üzerinde durulacak konular olacağını göstermektedir. Dolayısıyla siber güvenliğin ileride Maslow'un ihtiyaçlar hiyerarşisinde ifade ettiği güvenlik ihtiyacının önemli bir parçasını oluşturacağı söylenebilir. Siber saldırılara kamu ve askeri kuruluşların yanı sıra finans kuruluşlarının da çok fazla maruz kaldığı görülmektedir. Siber tehditlerle sık sık karşılaşılması ve yapı itibariyle karmaşık oluşu göz önüne alındığında, dünya çapında bankacılık sektöründe en önemli endişe kaynaklarından biri olmaktadır (Hassan, 2024). Fintek kuruluşları ve dijital bankacılığın getirdiği yeni teknolojik gelişmelere uyum sağlama baskısı, geleneksel bankacılık üzerinde büyük stres yaratmaktadır. Bu baskının temelini dijitale dönüşüm, yapay zekâ kullanımı ve siber güvenliği kabullenme konusundaki arzu ile müşteri veri güvenliği ve banka itibarını koruma arasında denge kurma zorunluluğuna dair kararların karmaşıklığı oluşturmaktadır (Rodrigues vd., 2022). Finansal sistemin önemli bir unsuru olarak faaliyet gösteren bankacılık sektöründe yukarıda ifade edilen nedenlerden dolayı siber güvenlik önemli bir yer tutmaktadır. Çünkü bankalar fon arz ve talebini buluşturan aracılık fonksiyonunu kredi kartı, ATM, internet bankacılığı, mobil bankacılık, telefon bankacılığı gibi araçlarla dijital platformlara taşıyarak (Korkmaz & Korkmaz, 2016) siber saldırıların hedefine oturmaktadır. Günümüzde dijital bankacılığın kullanımının artmasıyla birlikte bankacılık sektöründe siber suçların yıllar geçtikçe arttığı gözlenmektedir (Kumar, 2023). Dijital bankacılığın daha fazla evrimleşmesiyle büyük verinin yönetimi de daha kritik hale gelmektedir (Ghelani, 2022). Geniş bir toplumsal kitleye hizmet veren bankalar yapıları gereği çok çeşitli ve kıymetli evrak, belge, bilgi vb. veriyi depolamak ve işlemek durumundadırlar. Ayrıca birçok parasal işlem de gerçekleştirmektedirler. Bu duruma bağlı olarak söz konusu bu finansal işlemler sisteminin bütününün güvenliğini sağlaması beklenmektedir. Ülke ekonomilerinde finansal sistemin en temel kuruluşu sayılan bankaların güvenliğinin tasarruf sahibinden yatırımcıya, finansal aracılardan hükümetlere kadar birçok ekonomik paydaşın güvenliği anlamına geldiği de açıktır. Çünkü söz konusu olabilecek bir siber zafiyetin ekonominin tamamına sirayet etmesi ve yaygın hasarlara neden olması mümkün görünmektedir. Bankacılık sektörünün sağlıklı işleyebilmesinde güven mekanizmasının arz ettiği önem bilinmekle birlikte, dijitalleşen bankacılığın siber risklere maruz kaldığı ve kalacağı da bilinmektedir. Dolayısıyla sektörde siber güvenlik ile ilgili gerçekleştirilecek bütün süreçler politikalar ve uygulamalar önem arz etmektedir. Dijital bankacılık sistemleri

kullanıcılarına birçok gelişmiş kolaylık ve erişilebilirlik sağlasa da mevcut dijital işlemlerdeki siber güvenlik tehditlerinin ve gizlilik endişelerinin yaygınlaşması dijital bankacılığın benimsenmesinde en önemli engellerden birini oluşturmaktadır. Bu çalışmada bankacılık alanında siber güvenlik ile ilgili yapılan akademik çalışmaları bibliyometrik yöntemlerden yararlanarak incelemek, bankacılıkta siber güvenlik ile ilgili mevcut literatürü ortaya koyarak katkı sağlamak, çalışmaların tekrarlanmasını engelleyerek, çalışılmamış olan ve güncel konuları tespit edilmesi amaçlanmaktadır.

2. Bankacılık Sektöründe Siber Tehdit ve Siber Güvenlik

Yapay zekâ ve dijital dönüşüm alanlarında yapılan araştırmaların birçoğu teknolojinin hangi hızda, ne kadar ileri gidebileceği ve sonuçların ne olacağını anlama konusunda hala büyük zorluklarla karşılaşmaktadır. Geleneksel bankacılığın yapay zekâ ve bilgi teknolojilerinin getirdiği yeniliklerin benimsenmesinde önemli kazanımlara sahip olduğu bilinmektedir. Ancak bu geleneksel bankaların, dijital bankacılığın tüm avantajlarına eriştiği anlamına gelmemektedir (Rodrigues vd., 2022). Müşterilerin geleneksel bankalara olan sadakatinin yüksekliği ve teknoloji kullanımı kabulünün düşüklüğü ile müşteri yaş ortalamasının dijital bankacılık tercihi üzerindeki etkisi ve siber güvenlik sorunlarının varlığı gibi unsurlar bankacılığın geleneksel yapısının dönüşmesindeki yavaşlığı açıklamaktadır (Haksever & Baykal, 2023; Varol & İşler, 2024). Bu unsurlar aynı zamanda dijital bankacılığın zayıf kalmasının nedenleri arasında sıralanabilmektedir.

Bu sayılan eksikliklerin birçoğu pazarlama ve tutundurma çabalarıyla aşılabilir nitelikte görünmektedir. Ancak siber güvenlik yapısı itibariyle bunlardan ayrışmaktadır. Siber güvenliğin sistemi riske sokacak etkenler kadar dinamik olması ve teknolojik yenilikleri hızlı benimsemesi gerekmektedir. Aksi taktirde makrofinansal istikrarı bozucu bir süreç dahi gerçekleşebilir. Çünkü finans sektörünün karakteristik yapısı hassas verilere sahip olmak, yüksek konsantrasyon ve güçlü entegrasyonla açıklanmaktadır (IMF,2024).

Siber tehdit, yetki ve izni olmadan herhangi birinin dijital bankacılığına erişim sağlamaya çalışılan kötü niyetli bir eylem olarak tarif edilebilir (Kumar, 2023). Firmalar bu siber tehditlere 3 temel yönden maruz kalmaktadırlar (Bouveret, 2018) Bunlar;

- Gizlilik sorunları (özel bilgilerin 3. taraflara ifşası, ör: Veri ihlalleri nedeniyle itibar etkileri ve dava maliyetleri söz konusu olur)
- Bütünlük sorunları (sistemlerin kötüye kullanılması, ör: Dolandırıcılık nedeniyle doğrudan finansal kayıplara neden olunması)
- Erişebilirlilik sorunları (İş kesintileriyle ilgilidir, ör: Faaliyetlerin engellenmesiyle gelir kaybına neden olunması)
- Bulaşma sorunları (Veri ihlalleri ve dolandırıcılık faaliyetlerinin kısa vadeli bulaşmaya sebep olması)

Küresel boyutta siber suçların neden olduğu maliyetlerin saniyede 190 dolar, günde 16 milyar dolar ve ayda 500 milyar dolar civarında olduğu tahmin edilmektedir (Cele & Kwenda, 2024). ORX (üyelerine rapor sunan bir kuruluş) haberleri ve IMF (International Monetary Fund) hesaplamalarına göre 2009-2017 yılları arasında siber saldırıların %43'ünü dolandırıcılık, %34'ünü veri ihlalleri ve %23'ünü iş kesintileri oluşturmaktadır. İş kesintileri hemen farkedilmesine ragmen diğer siber saldırılar geç farkedilebilmektedir. Bu saldırıların ana hedefi gelişmiş ülkeler olmakla birlikte gelişmekteki ülkelerde de saldırılar görülmektedir. Olayların %39'u ABD'de, %7'si İngiltere'de, %6'sı Rusya'da, %4'ü Çin'de ve %3'ü Hindistan'da gerçekleşmektedir. Ayrıca finansal kuruluşlara yapılan saldırıların %91'i bankalara, %7'si sigorta şirketlerine yönelik olmuştur (Bouveret, 2018). Günümüzde yaşanan birçok siber olayın artmasına çeşitli faktörler sebep olmaktadır. Bu faktörlerin başında teknolojiye artan bağlılık, finansal inavosyon gelişmeleri, Covid-19 salgını ve jeopolitik gerilimler (Rusya'nın Ukrayna'yı işgali sonrası vb.) sayılabilir (IMF, 2024).

Bankacılığının dijitalleşmesi ile birlikte ortaya çıkan güvenlik sorunlarından birçok önleyici tedbire rağmen emin olunamamaktadır. Söz konusu bu sorunlar ve çözüm önerileri aşağıdaki tabloda ifade edilmektedir (Alzoubi vd., 2022).

Tablo 1. Dijital Bankacılıkta Karşılaşılan Çeşitli Güvenlik Sorunları ve Çözümleri

Sorunlar	Çözümler
Şifrelenmemiş veriler	Dijital sertifikaların verilmesi
Kötü amaçlı yazılım	OTP tokenleri
Güvenilmez üçüncü taraf hizmetleri	Tarayıcı koruması
Manipüle edilmiş veriler	Cihaz tanımlama
Sahtecilik	İşlemsel izleme

Kaynak: (Alzoubi vd., 2022).

Yukarıdaki tabloda görüldüğü üzere dijital bankacılıkta siber güvenlik tehditleri olarak karşımıza çıkan sorunların başında şifrelenmemiş veriler, kötü amaçlı yazılım, üçüncü taraf hizmetleri, sahtecilik, kimlik avı gibi birçok tehditler gelmektedir. Bu tehditlerin dijital bankacılıkta siber güvenlik eksikliği, farkındalık eksikliği, yetersiz bütçe, yönetim eksikliği, zayıf kimlik ve erişim yönetimi, fidye yazılımlarının yükselişi, mobil cihazlar ve uygulamalarından kaynaklandığı görülmektedir. Özellikle kimlik avı ve kimlik hırsızlığı dijital bankacılığın benimsenmesini engelleyen en önemli siber tehditler olarak belirtilmektedir (Cele & Kwenda, 2024). Dijital bankacılıkta yukarıdaki tabloda ifade edilen çözümlere ek olarak; entegre güvenlik önlemlerinin alınması, şifrelenmiş verinin kullanılması, bilginin korunması, anti virüs kullanımı, tüketici farkındalığının arttırılması, makine öğrenimi ve büyük veri analitiğinin kullanımı ile güvenliğinin öneminin anlaşılması gibi hususlar da sıralanabilmektedir (Kumar, 2023). Bu sayılan çözüm önerilerinin en iyi optimizasyon teknikleri olarak kullanımı hassas verilerin davetsiz misafirlerden korunmasına yardımcı olacaktır (Ghelani, 2022). Unutulmamalıdır ki siber güvenliğin geleceği siber saldırılar gerçekleşmeden onu durdurmaktan geçmektedir (Unit21, 2022). Dahası gelişmiş siber güvenlik farkındalığı ve bilgi paylaşımını teşvik eden bir ekosistem, daha güvenli ve daha dayanıklı dijital bankacılığa önemli sayılabilecek katkılarda bulunabilir (Cele & Kwenda, 2024). Bu noktada IMF tarafından Siber Risk Denetim Araç Seti geliştirilmiştir. Bu risk seti, model yönetmelik, bir risk değerlendirme aracı, bir denetim süreci belgesi ve bir denetim el kitabından oluşmaktadır. Bunun yanı sıra IMF, Basel Bankacılık Denetim Komitesi, Finansal İstikrar Kurulu ve Uluslararası Menkul Kıymetler Komisyonları Örgütü gibi standart belirleyici kuruluşların çabalarına katkıda bulunarak siberle ilgili uluslararası düzeydeki politikaların geliştirilmesinde önemli bir rol üstlenmektedir (IMF, 2024).

3. Yöntem

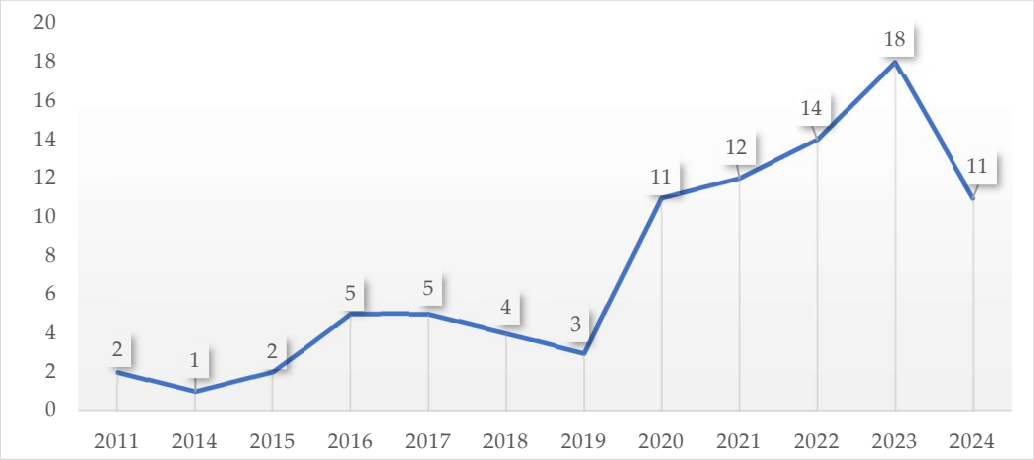
Günümüzün dijital çağında, bankacılık sektörü teknolojik gelişmelerle birlikte büyük bir dönüşüm yaşamaktadır. İnternet bankacılığı, mobil uygulamalar ve dijital ödeme sistemleri gibi yenilikler, finansal hizmetlere erişimi kolaylaştırmıştır. Bu dijitalleşme süreci aynı zamanda siber güvenlik risklerini de ortaya çıkarmıştır. Bankacılık sektöründe siber güvenliğin önemi, hem finansal kuruluşların hem de müşterilerin varlıklarını ve hassas bilgilerini koruma ihtiyacına dayanmaktadır. Bu bağlamda çalışmanın konusunu bankacılıkta siber güvenlik oluşturmaktadır. Bu alandaki akademik çalışmaları inceleyerek literatüre katkı sağlamak ve çalışmaların tekrarlanmasını engellemek amacıyla bibliyometrik yöntemlerden yararlanılmıştır.

Bibliyometrik analiz gelişmekte olan ilgili literatürün hacimsel ve büyüklük bakımından belirlenmesine imkan veren, nicel bir metodoloji olarak karşımıza çıkmaktadır. Odak bir alanda yayınlanmış akademik katkıları irdeleyerek literatürü retrospektif bir şekilde ele alan bu yöntemde, genelde bibliyometrik performans analizi (yayınların ülke, yıl, yazar, bağlı kuruluş vb. şekilde değerlendirilmesi) ve bilim

haritalama (ilişkisel bibliyometrik de denilen bu yöntemde yayınlar arasındaki ilişkileri kapsayan ortak yazar, ortak atıf, ortak kelime analizi vb.) teknikleri benimsenmektedir (Guleria & Kaur, 2021). Araştırmanın temel amacı, bankacılık sektöründe siber güvenlik üzerine yapılan çalışmaların bibliyometrik analizi yapılarak literatürdeki boşlukların tespit edilmesi ve güncel çalışma konularının belirlenmesidir. Birçok bibliyometrik analizin veri kaynağını WoS ve Scopus gibi veri tabanı oluşturmaktadır (Mongeon & Paul-Hus, 2016). Bu kapsamda bibliyometrik analiz yapmak için Web of Science (WoS) veri tabanı tercih edilmiştir. WoS'un erişim platformu ve veritabanı olarak seçilmesinin temel nedeni, WoS veritabanının literatür incelemelerindeki temsiliyetinin birçok bibliyometrik çalışmada doğrulanmış olması (Ateş vd., 2024) ve neredeyse tüm önemli araştırma makalelerini içermesidir (Qiao vd., 2021). WoS veri tabanında 24.10.2024 tarihinde "cyber security" ve "banking" arama terimleri kullanılarak tarama yapılmıştır. Bu tarama sonucunda 171 sonuç çıkmış ve sonuçlara yönelik sadece araştırma makalesi tercih edilerek filtreleme yapılmış ve 88 araştırma makalesinden veri seti oluşturulmuştur. Belge türü açısından, analiz edilen literatürün standartlaştırılmış veri formatlarına sahip olmasını sağlamak için çalışma araştırma makaleleri ile sınırlandırılmıştır. Ancak belge türlerinin bu seçimi, diğer kaynaklardan elde edilen bilgilerin kapsamını da sınırlandıra bilmektedir. Gelecekteki araştırmalar, en son gelişmeleri ve daha çeşitli bulguları yakalamak için bildiri gibi diğer belge türlerini de dahil etmeyi düşünebilirler (Huang vd., 2024). Bibliyometrik analizler VOSviewer ve Bibliometrix programları kullanılarak gerçekleştirilmiştir.

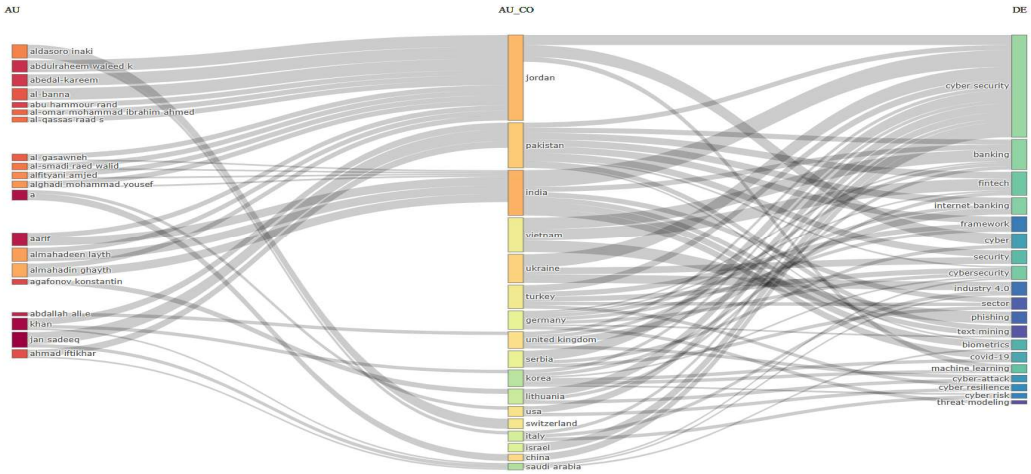
4. Bulgular

Bu bölümde VOSviewer ve Bibliometrix programları kullanılarak yapılan analizlerin grafikleri ve ilişki ağları oluşturularak yorumlanmıştır. Araştırma kapsamında incelenen 88 araştırma makalesinin 9'u tek yazarlı geri kalanı ise çok yazarlıdır. Yayınların yıllık büyüme ortalaması yaklaşık %17,35 olarak hesaplanmıştır. Araştırma makalesi başına düşen ortalama atıf sayısı ise 10'dur.



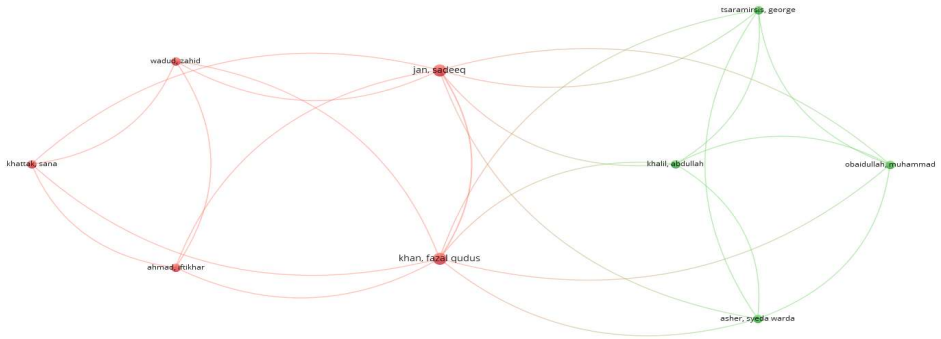
Grafik 1. Bankacılıkta Siber Güvenlik İle İlgili Yayınların Yıllara Göre Dağılımları

Bibliyometrik analiz için oluşturulan veri seti incelendiğinde en eski çalışmanın 2011 yılında yapıldığı tespit edilmiştir. Bu durum aynı zamanda konunun güncel bir konu olduğunu da göstermektedir. 2011 yılı ile 2020 yılları arasında araştırma makalelerinin sayısının oldukça az olduğu görülmektedir. 2020 yılı itibariyle dijitalleşmenin hız kazanması mobil uygulamaların artması ve özellikle Covid-19 salgını dolayısıyla internet tabanlı mobil teknolojilerin gelişmesi ve temassız teknolojilerin zorunlu kullanımı güvenlik ile ilgili sorunları ortaya çıkarmıştır. Yayınların sayısının artmasında bu durumun etkili olduğu düşünülmektedir.



Şekil 1. Bankacılıkta Siber Güvenlik İle İlgili Yazar, Ülke ve Anahtar Kelimelere Yönelik İlişki Ağının Görselleştirilmesi

Yazarlar, ülkeler ve kullanılan anahtar kelimelerin birlikte yer aldığı Şekil incelendiğinde en fazla farklı yazara sahip olan ülke Ürdün ve Pakistan olmuştur. Arama terimleri olan siber güvenlik ve bankacılık terimleri dışında ön plana çıkan anahtar kelimeler ise, fintek, internet bankacılığı, metin madenciliği, siber saldırı, siber risk, makine öğrenimi, kimlik avı (dolandırıcılık) ve siber dayanıklılıktır. Bankacılık sektöründe siber güvenlik ile ilgili en fazla farklı konuyu çalışan ülke ise Pakistan olmuştur.



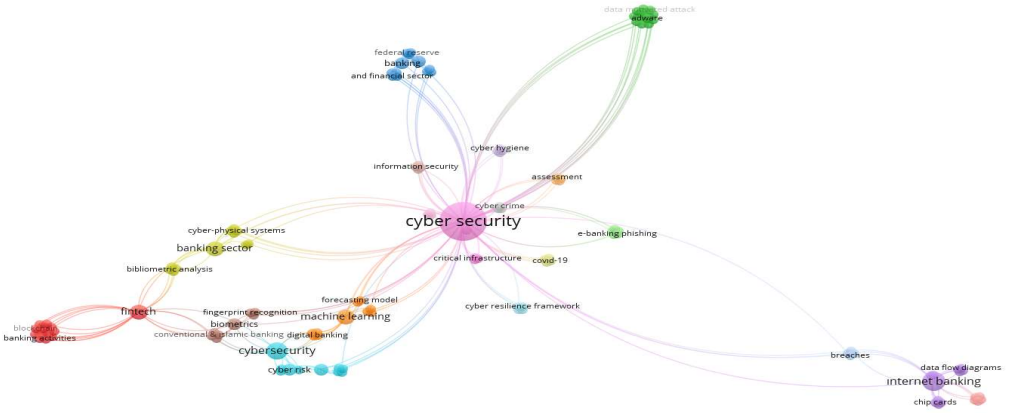
Şekil 2. Bankacılıkta Siber Güvenlik İle İlgili Yayınlardaki Yazarların Görselleştirilmesi

İncelenen araştırma makalelerinde toplamda 169 yazar bulunmaktadır. Çalışma kapsamında incelenen araştırma makalelerinin yaklaşık %34'ü uluslararası ortak yazarlı çalışmalardan oluşmaktadır. Araştırma makalesi başına ortalama yazar sayısı yaklaşık 3,42 olarak hesaplanmıştır.

Yazarların yayın sayıları incelendiğinde Sadeeq Jan ve Fazal Qudus Khan'ın 2'şer yayını diğer yazarların ise 1'er yayını bulunduğu görülmektedir. En fazla atıf alan yazarlar incelendiğinde ise, B. Shravan Kumar (143), Vadlamani Ravi (143), Yasmeen Hanif (47), Harjinder Singh Lallie (47), Dinh Tran Ngoc Huy (34), Sylwia Gwozdziewicz (34), Hoang Thi My Hanh (34), Le Thi Thu Huogn (34), Luong Thi Yen Nga (34), Nguyen Ngoc Thach (34), Vu Quynh Nam (34), Kıymet Caliyurt (32), Sezer Bozkuş Kahyaoğlu (32) olmuştur. Bankacılıkta siber güvenlik ile ilgili olarak en etkili yazarlar ise, Sadeeq Jan, Fazal Qudus Khan, Sylwia Gwozdziewich, Hoang Thi My Hanh, Le Thi Thu Huong'dur.

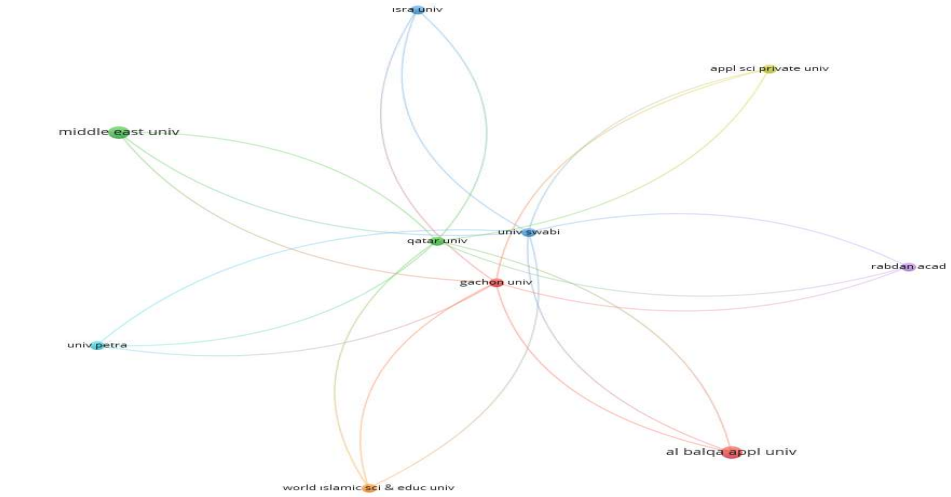
Şekil 3. Bankacılıkta Siber Güvenlik İle İlgili Yayınların Ülkelere Göre Görselleştirilmesi

Yayınların ülkelerine yönelik analiz yapılmış ve 88 araştırma makalesinde toplamda 32 farklı ülke olduğu tespit edilmiştir. Yayınların ülkelere göre dağılımı incelendiğinde en fazla yayın yapan ülke sırasıyla Hindistan (9), Pakistan (5), Ürdün (5), ABD (4), İngiltere (4) olmuştur. En fazla atıf alan ülkeler incelendiğinde Hindistan (170), İngiltere (54), Güney Kore (40), ABD (38), İtalya (36), Japonya (34), Polonya (34), Vietnam (34), Türkiye (33) atıf almışlardır.



Şekil 4. Bankacılıkta Siber Güvenlik İle İlgili Yayınlardaki Anahtar Kelimeler Arasındaki İlişkilerin Görselleştirilmesi

Şekil incelendiğinde siber güvenlik, internet bankacılığı, bankacılık sektörü, makine öğrenimi, biyometrik, siber saldırı, metin madenciliği, reklam yazılımı, bankacılık aktiviteleri, bankacılık virüsleri, blokzincir, tıklama dolandırıcılığı, bulut teknolojileri, siber güvenlik riski yönetimi, veriye dayalı saldırı gibi anahtar kelimelerin ön plana çıktığı görülmektedir. Anahtar kelimelerin aralarındaki ilişkiler incelendiğinde siber güvenlik ile siber saldırı, virüsler, tıklama dolandırıcılığı ve risk yönetimi anahtar kelimeleri en fazla ilişkili olan kelimelerdir. Bu durum aynı zamanda siber güvenlik üzerine yapılan çalışmaların önemini yansıtmaktadır. Diğer anahtar kelimeler incelendiğinde ise, siber güvenliği sağlamada veya artırmada kullanılan makine öğrenimi, blokzincir ve risk yönetimi anahtar kelimeleri ön plana çıkmaktadır.



Şekil 5. Bankacılıkta Siber Güvenlik İle İlgili Yayınların Organizasyonlar Arasındaki İlişkilerin Görselleştirilmesi

Yazarların kurumları incelendiğinde ise etki düzeyi en yüksek olan kurumlar sırasıyla Gachon Univ., Qatar Univ., Univ. Swabi, Al Balqa Appl Univ., Appl Sci Private Univ., Middle East Univ. olmuştur.

Şekil 6. Bankacılıkta Siber Güvenlik İle İlgili Yayınların Başlıklarına Yönelik Kelime Bulutu

Çalışma kapsamında incelenen 88 araştırma makalesinin konu başlıklarına yönelik kelime bulutu oluşturulmuştur. Kelime bulutuna göre ön plana çıkan metalar ise, bilgi güvenliği, bankacılık, sistem, önyargılar, anormallik tespiti, siber güvenlik, ticaret, saldırı tespiti, başarı, kurumsal sosyal sorumluluk, performans, şema, üst yönetim ekibi, teknoloji kabulü, siber güvenlik ifşası, ekonomik büyüme, güvence, parmak izi, güvenlik açığı, derin öğrenme yaklaşımı, kart dolandırıcılığı tespiti, müşteri deneyimi, sezgisel yöntemler, kriptografi, risk alma, risk, etki, yönetim gibi kelimelerden olmaktadır. Yayınlara genel olarak bakıldığında ön plana çıkan yayınlar Kumar & Ravi (2016), Hanif & Lallie (2021), Thach vd. (2021), Bozkuş Kahyaoğlu & Caliyurt (2018), Vishwanath vd. (2020) çalışmalarıdır. Yapılan analiz sonucunda etki düzeyi en yüksek olan yayınların ise Khan vd. (2023), Karim vd. (2024) tarafından yapılan çalışmalar olduğu tespit edilmiştir. Söz konusu bu çalışmalar ile ilgili açıklayıcı bilgiler aşağıdaki gibidir.

Kumar & Ravi (2016) "A survey of the applications of text mining in financial domain" adlı çalışmalarında, metin madenciliğinin çeşitli finansal uygulamaları ile ilgilenen araştırmaları ele almışlardır. Çalışmada bu uygulamalar arasında FOREX Oranı Tahmini, Borsa Tahmini, Müşteri İlişkileri Yönetimi (CRM), Müşteri Kaybı Tahmini ile Siber Güvenlik, Kimlik Avı Tespiti, Spam Tespiti, Kötü Amaçlı Yazılım Tespiti, Sahtekarlık Tespiti ve Saldırı Tespiti'nin yer aldığı ifade edilerek veriyi işlemek ve tahmin

etmek için daha verimli tekniklerin geliştirilmesini gerektiğini vurgulanmaktadır. Çalışmada sayısal verileri metinsel verilerle birleştirmenin daha iyi tahminler üretmede yardımcı olacağının altı çizilmekle birlikte, saldırı tespiti ve dolandırıcılık tespitinin nadiren metin madenciliği yaklaşımlarıyla ele alındığı belirtilmektedir. Ayrıca her alanda (finans, sigortacılık vb.) ontolojilerin oluşturulması gerekliliği de çalışmada ifade edilmiştir.

Bozkuş Kahyaoglu & Caliyurt (2018) "Cyber security assurance process from the internal audit perspective" adlı çalışmalarında iç denetim ve risk yönetimi bakış açısıyla siber güvenlikte temel sorunlar ve zayıflıklara değinerek, siber güvenlik yaklaşımlarını analiz etmeye çalışmışlardır. Çalışmada siber odaklı 4 büyük standart çerçevenin varlığından bahsederek, örnek bir siber güvenlik farkındalık kontrol listesi sunmaktadırlar.

Vishwanath vd. (2020) "Cyber hygiene: The concept, its measure, and its initial tests" adlı çalışmalarında, siber hijyen kavramını işlevselleştirerek altboyutlarına ayırmışlardır. Araştırma ile 5 alt boyuttan ve 18 öğeden oluşan siber hijyen için bir ölçek geliştirilmiştir. Ölçek aracılığıyla kullanıcıların teknoloji ile ilgili öz inançları, çevrimiçi bilgileri bilişsel açıdan nasıl işledikleri ile çevrimiçi bankacılıkta dâhil olmak üzere insan siber etkileşiminin yönlerini ortaya koymaya çalışmaktadırlar.

Thach vd. (2021) "Technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam" adlı çalışmalarında, gelişmekte olan ülkelerde riskler ve azaltma önlemleri üzerinde durarak, endüstri 4.0'da risk yönetimi ve siber güvenlik konularını ele almaktadırlar. Çalışmada dijital bankacılığın ekonomik etkinliği arttıracağı ancak yasal çerçevenin geliştirilmesi ve bilgi iletişim teknolojilerine uygun olması ile siber güvenlik ve risk yönetiminin uluslararası standartlara sürekli olarak eşleştirilmesi gerekliliklerine değinilmektedir.

Hanif & Lallie (2021) "Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust" adlı çalışmalarında Birleşik Krallık'ta 55 yaş ve üzeri kişilerde mobil bankacılık uygulamalarını kullanma niyeti üzerinde siber güvenlik faktörlerinin etkisini ölçmek için kullanılabilecek bir model önermektedirler. Çalışma ile Birleşik Krallık'ta 55 yaş ve üzeri kişilerde mobil bankacılık uygulamalarını kullanma niyetinin ana belirleyicilerinin performans beklentisi ve ardından algılanan siber güvenlik riski olduğu ifade edilmektedir.

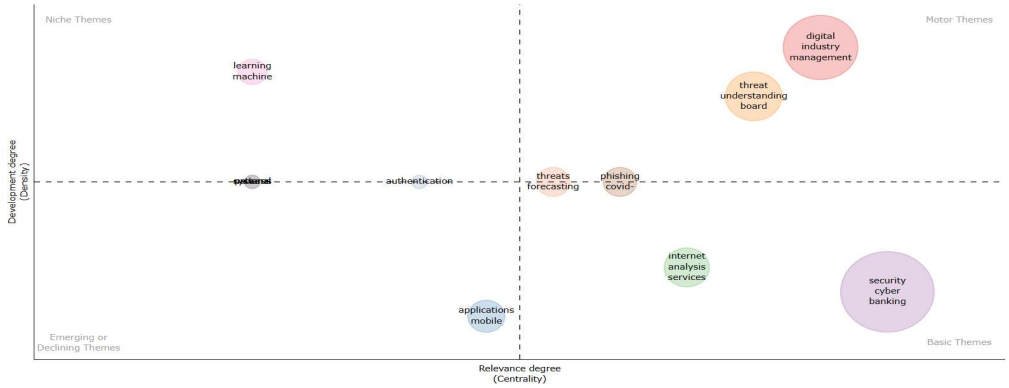
Kumar (2023) "An overview of cyber security in digital banking Sector" adlı çalışmasında, bankacılık sektörünün diğer sektörlere göre daha fazla siber saldırıyla karşı karşıya kaldığını ifade ederek, bankacılık sektöründeki siber saldırılara karşı siber güvenlik sağlama yollarını ele almaktadır. Çalışmada dijital ve çevrimiçi bankacılıkta Integrated SecurityAsBFSI (Breath First Search Integrated) teknolojisinin bankacılıkta tüm bileşenlerin birlikte çalıştığı ve iletişim kurduğu entegre güvenlik için yüksek düzeyde düzenlenmiş en iyi ve faydalı teknoloji olduğuna vurgu yapılmıştır. Siber güvenliğin önemi ve riskinin analiz edilmesi gerektiğine değinilen çalışmada özellikle tüketici farkındalığının arttırılması, kötü amaçlı yazılımdan koruma uygulamalarının kullanılması ve çeşitli cihazlarda ve bulutta tutulan verilerin şifrelenmesi gerektiği ifade edilmiştir.

Khan vd. (2023) "Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis" adlı çalışmalarında, siber güvenlik riskine karşı koymak ve bankacılık sektörüne yüksek güvenlik ve emniyet sağlamak için geleneksel ve İslami bankacılıkta biyometri sisteminin temel özelliklerini ayrıntılı olarak açıklamaktadırlar.

Çalışmada siber güvenliğin tek bir otorite tarafından ele almasının gerekliliği ve kimlik doğrulaması için en güvenilir ve etkili yöntemin fiziksel güvenlik (biyometrik) yöntemleri olduğu ifade edilmektedir.

Karim vd. (2024) "Online Banking User Authentication Methods: A Systematic Literature Review" adlı çalışmalarında, çevrim içi bankacılıkta kullanılan son teknoloji

kimlik doğrulama yöntemlerini ve potansiyel siber tehditleri gözden geçirmektedirler. Çalışmada bilgi tabanlı kimlik doğrulama, biyometrik kimlik doğrulama, sahiplik tabanlı kimlik doğrulama ve diğer yöntemler karşılaştırılarak bu yöntemlerin avantaj ve dezavantajları ortaya konmaya çalışılmıştır. Çalışma ile önde gelen finansal kuruluşların kimlik doğrulamada en iyi uygulamaları karşılaştırılmış ve sonuç olarak iki faktörlü kimlik doğrulama ve çok faktörlü kimlik doğrulama yöntemlerinin çevrimiçi güvenliği arttırmaya yardımcı olacağı tespit edilmiştir. Ayrıca çalışma ile yeni siber zorlukların ortaya çıkacağı ve finansal kuruluşlar ile tüketicilerin tetikte olmaları gerektiği vurgulanmıştır.



Şekil 7. Yayınlara Yönelik Tematik Harita

Çalışmada incelenen makaleler için oluşturulan tematik haritada niş temalar, hareketli temalar, temel temalar ve azalan temalar olarak değerlendirilmiştir:

Niş temalarda öne çıkan konular: Öğrenme, makine öğrenimi, kimlik doğrulama

Hareketli temalarda öne çıkan konular: Yönetim, dijital bankacılık, etkiler, risk, siber güvenlik, aktiviteler, farkındalık, tespit

Temel temalarda öne çıkan konular: Siber güvenlik, bankacılık, finans, geliştirme, öğrenme, analiz, internet hizmetleri, tehditler, tahmin, kimlik avı, Covid-19

Azalan temalar: Mobil uygulamalar, kullanıcı deneyimi, değerlendirme, performans

Temalar incelendiğinde çalışmanın anahtar kelimesini oluşturan siber güvenlik konusu hem temel temalarda hemde hareketli temalarda yer almaktadır. Bu durum aynı zamanda siber güvenlik ile ilgili çalışmaların güncel olduğunu göstermektedir. Güncel konular arasında risk yönetimi, kullanıcıların farkındalıklarını belirlemeye yönelik çalışmalar, siber güvenlik ile kullanıcıları bilinçlendirmeye yönelik aktiviteler ve kullanıcıların siber güvenliğe yönelik bilinçlendirme konuları ön plana çıkmaktadır. Azalan temalar incelendiğinde mobil bankacılık ve mobil bankacılığın kullanım deneyimleri üzerine çalışmalar ön plana çıkmaktadır. Covid 19 döneminde yaşanan kısıtlamalara bağlı olarak zorunlu bir biçimde bireyler dijitalleşmeye yönelmiş ve bu durum beraberinde güvenlik açıkları, dolandırıcılık yöntemleri konusunda mevcut sistem yetersiz kalmıştır. Bu noktada niş temalar incelendiğinde temassız ödeme yöntemleri ve kullanıcı deneyimleri, güvenlik açıklarına karşı kimlik doğrulama yöntemleri, kullanıcı deneyimleri, güvenlik ve siber güvenlik ile ilgili olarak makine öğrenimi konuları ön plana çıkmaktadır. Azalan temalarda mobil bankacılık uygulamaları ve deneyimleri yer alırken, niş temalarda kimlik doğrulama ve temassız kullanımlar ve deneyimler yer almaktadır. Çalışma konuları incelendiğinde Covid-19 dönemi sonrası siber güvenlik çalışmalarının sayısı oldukça artmıştır.

5. Sonuç ve Öneriler

2020 yılı itibariyle dijitalleşmenin hız kazanması mobil uygulamaların artması ve özellikle Covid-19 salgını dolayısıyla internet tabanlı mobil teknolojilerin gelişmesi ve temassız teknolojilerin zorunlu kullanımı güvenlik ile ilgili sorunları ortaya çıkarmıştır.

Dolayısıyla yapılan literatür incelemesinde yayın sayılarının 2019 yılı sonrasında artmasında bu durumun etkili olduğu düşünülmektedir. Çalışmalarda ön plana çıkan anahtar kelimeler incelendiğinde siber güvenlik ve fintek uygulamaları ile ilgili kavramların daha çok ele alındığı görülmektedir. Gelişen teknoloji ile artan dijitalleşme sonucu finansal teknoloji uygulamalarının yaygın kullanımı dolayısıyla çokça yaşanan siber güvenlik ihlal vakaları bu alanlarda akademik ilgiyi de beraberinde getirmiştir. Teknolojik gelişimin en son geldiği nokta olarak ifade edilen dijitalleşme, bankacılık sektörüne yeni fırsatlar sunarken önemli siber güvenlik ihlalleriyle de karşı karşıya bırakmaktadır. Davetsiz ziyaretçiler sebebiyle çeşitli tehditlere maruz kalan finans sektörü ve paydaşları bu süreçten sadece para ve zaman kaybederek çıkmamakta aynı zamanda kredi sektörü için her şey anlamına gelebilecek itibarlarını da kaybetme durumunda kalmaktadırlar. Banka için itibar, müşteri, yatırımcı ve bütün toplumun gözünde saygınlık, güven, kalite, memnuniyet, imaj, vb. faktörlerin kombinasyonu olduğu için finansal hedeflere ulaşmaya ve performansa önemli katkı sağlamakta ve sektördeki bankanın başarısını da olumlu etkilemektedir (Korkmaz vd., 2023). Bugün gelinen nokta itibariyle sektörde mevcut siber güvenlik çerçevelerinin etkinliği kritik bir endişe kaynağı olarak ortaya çıkmaktadır. Katmanlı siber güvenlik savunmasının ilk aşamasını bile başarı ile faaliyete geçirmemiş kurumların açıkları, siber güvenlik saldırıları için kolayca hedef olabilmektedir. Güvenlik riske verilen bir cevaptır. Dolayısıyla siber riskler değerlendirilmelidir. Bu değerlendirilmedeki en kritik aşama ise önem arz eden değerli varlık, bilgi ve belgelere ilişkin tehdit ve risklerin belirlenerek ana hatlarıyla ortaya konulmasıdır (Babu, 2018). Bankacılıkta bu endişelerin giderilmesi ve sağlıklı bir iyileştirme için benimsenmiş bir risk değerlendirme metodolojisinin varlığı, gelişmiş sağlam bir siber güvenlik kültürü, çalışanlar ve müşterilerde yüksek siber güvenlik farkındalığı ve düzenleyici zorunluluklara yüksek uyum gibi çeşitli faktörler önem taşımaktadır (Oyewole vd., 2024). Siber güvenlik kabiliyetini azaltan temel faktörlerin başında ise gelişmiş teknoloji eksikliği ve yasal uyumun yetersiz oluşu gelmektedir (Whang vd., 2020). Siber güvenlik ihlallerinin temel motivasyon kaynağının para olduğu bilinmektedir. Dolayısıyla siber suçlar için finansal kuruluşlar ve paydaşları çeşitli fidye yazılımlar, kimlik avı vb. yöntemlerle favori hedefler haline gelmektedir (Babu, 2018). Siber güvenlik ihlallerini önlemek için bankalar siber güvenlik risklerini azaltma sorumluluğunu daha fazla almalıdırlar (Alghazo vd., 2017). Çünkü finansal tüketicilerin çok çeşitli kaynaklardan finansal ürün ve hizmetlere erişim sağladıkları bilinmektedir. Bu erişim noktalarından gelen tehditleri yönetmeleri de kurumsal yapılara göre daha zor olabilmektedir (Babu, 2018). Siber tehditlerle mücadele etmek zorlu bir durum olarak karşımıza çıkmaktadır. Çünkü bu süreç teknoloji ile kendini sürekli yenileyen ve başa çıkılması için farklı alanlarda (bilgi teknolojileri, finans, vb.) beceri ve uzmanlıklar gerektiren sofistike bir yapıdır. Finans sektöründe bulaşıcılık riskinin yüksekliği siber tehditler içinde geçerli olmakta ve sistemik etkilerle tüm finansal siteme sirayet ederek istikrarı bozucu bir hal alabilmektedir. Bu nedenle düzenleyici ve denetleyici otoriteler siber güvenlik seviyelerinin arttırılması ve yönetişim kontrollerinin güçlendirilmesini teşvik etmeye çalışmaktadırlar (Birindelli & Iannuzzi, 2024). Siber ihlaller doğası gereği uzaktan erişimi kapsadığından gelişen tehdidin boyutu da sınır ötesi olabilmektedir. Dolayısıyla siber güvenlik ihlallerinin giderilmesini, sadece bir banka boyutuyla ele alma hatasına düşmeden, uluslararası bir çerçevede dayanıklılığı ve işbirliğini arttırıcı yasal düzenlemeler önem arz etmektedir (Mahboob vd., 2023). Siber stres testlerinin ve tek tip siber risk protokollerinin ortaya çıkması gibi güncel girişimlerin varlığı bu yönde ilerlemenin olduğunu göstermektedir. Riski yönetmenin ve sistemik etkilerini azaltmanın en iyi yolu hiç şüphesiz teşhis, ölçüm ve sınırlama araçlarını oluşturmaktan geçmektedir (Birindelli & Iannuzzi, 2024). Unutulmamalıdır ki işletmeler yaşayan birer sistemlerdir. Bankalar ne kadar dijitalleşseler de beşeri sermayesi kabiliyetinde fark yaratmaları mümkün olabilir. Gelenekselden dijitale dönüşen süreçler ve sistemlerde çalışanların dijital sistemleri kullanma kabiliyetinin arttırılması bu noktada etkili olabilecek unsurlar arasında sıralanabilir (Nurjannah, 2023). Ayrıca siber güvenlik

şirketlerinin de bankalarla yakın çalışarak siber tehditlerin önünde kalıp proaktif bir rol üstlenmeleri gerekmektedir. Bu rol tam kapsamlı siber güvenlik hizmetleri sağlama adına önemlidir. Tehditleri algılamada ve önlemede güçlü, müdahale süreçlerinde etkili, sık denetim ve kapsamlı personel eğitimi ile bankacılık ekosisteminin siber ihlallere karşı iyileştirilmesi mümkün kılınabilir (Asmar & Tugan, 2024). Dijital dönüşüm esas itibariyle çok önemli kazanımları getirmektedir. Performansın geliştirilmesi ve tüketici davranışları konusunda ki fırsatlar buna örnek verilebilir. Ancak teknolojik yeniliklerin kurumsal yapıdaki değişiklikleri de zaruri kılması çeşitli zorlukları da beraberinde getirmektedir. Elbette ki bilgisayar otomasyon sistemlerini çeyrek asırdan fazladır kullanan finans sektörü için siber risk yönetimi yeni bir olgu değildir. Ancak sağlam ve kapsamlı bir siber risk yönetim stratejisi hiç bu kadar kritik öneme sahip olmamıştır. Dahası finansal sektör kuruluşları dijital ayak izlerini genişlettikçe bu önem giderek artacağa benzemektedir (Atkins vd., 2024). Nihayetinde dijital bankacılık için dijital stratejik planların varlığı ve uygulamaya konması geleceğin bankalarına bugünden rehberlik edebilir (Nurjannah, 2023). Dolayısıyla finansal sektör kuruluşları ileri teknoloji ürünlerini istekli bir şekilde benimserken, siber risklerin artmasına yönelik şimdiden harekete geçmelilerdir. Bu aksiyon çevreyi geleceğe hazır hale getirmek adına yapılmalıdır. Unutulmamalıdır ki bugünün trend teknolojileri yarın için değişebilmekte ve eskiyebilmektedir.

Yukarıda detaylandırılmış öne çıkan çalışmaların ifade ettiği üzere siber güvenlikte kimlik doğrulamanın (biyometrik, ikili, çoklu vb.) sektör için önemli olduğu ön plana çıkmaktadır. Ayrıca Integrated SecurityAsBFSI (Breath First Search Integrated) teknolojisinin bankacılıkta tüm bileşenlerin birlikte çalıştığı ve iletişim kurduğu entegre güvenlik için yüksek düzeyde düzenlenmiş en iyi ve faydalı bir teknoloji olduğu literatürde ifade edilerek, finansal kuruluşlar için uygulanabilir bir öneri olarak sunulduğu görülmektedir.

Yine bankacılıkta siber güvenlikle ilgili literatürde öne çıkan çalışmalar irdelendiğinde, çalışmaların ülkelere özgü olduğu görülmektedir. Başka bir ifadeyle ülkelerin problemleri ve ihtiyaçlarına çözüm bulmak adına yayınların odağının çeşitlendiği görülmektedir. Örneğin Thach vd. (2021), Vietnam özelinde gelişmekte olan ülkelerin siber güvenliğine değinirken, Hanif & Lallie (2021), Birleşik Krallık'ta 55 yaş ve üzeri kişilerde mobil bankacılık uygulamalarını kullanma niyeti üzerinde siber güvenlik faktörlerinin etkisini ölçmek ile ilgilenmişlerdir. Vietnam gelişmekte olan bir ülke olarak siber güvenliğe çare ararken, Birleşik Krallık'ların yaşlı nufusu nedeniyle siber güvenliği ele almakta olduğu görülmektedir. Bu yaklaşımla Türkiye'de bankacılıkta siber güvenlik konusu genç nufus ve gelişmekte olan ülke dinamikleri göz önünde bulundurularak ele alınabilir. Özellikle genç nufusun son dönemde sermaye piyasalarına katılımı ve kripto para uygulamalarına olan rağbeti göz önüne alındığında Türkiye'de siber güvenlik, mali suçlar ve terörün finansmanı ile finansal okuryazarlık konularını içerecek şekilde birlikte ele alınabileceği söylenebilir.

Söz konusu çalışmaların kamu ve sektör otoritelerine; siber güvenlik farkındalık listeleri ile finansal alanda ontolojinin geliştirilmesini önermekte oldukları da görülmektedir. Ayrıca araştırmalarda insan-siber etkileşimi ile ilgili daha fazla çalışmanın yapılabileceği de ifade edilmiştir.

Genel olarak bakıldığında bankacılık ile iligili güçlü güvenlik tekniklerinin uygulanması ve müşteriler arasında eğitim ve farkındalığın artırılması oldukça önemli bir hale geldiği çalışmalarda belirtilmiştir. İncelenen çalışmalarda kullanıcılara yönelik olarak; siber güvenlik ile ilgili eğitim ve öğretim girişimleri yapılarak güvenilir ve güncel güvenlik sistemlerinin benimsenmesini sağlanması önerilmiştir. Bir başka ifadeyle tüm paydaşalar ile kullanıcılar arasında gelişmiş siber güvenlik farkındalığı ve bilgi paylaşım uygulamalarını teşvik ederek, daha güvenli ve daha dayanıklı bir dijital bankacılık ortamı oluşturulması gerekmekte ve bu konuda çalışmaların yapılması önerilmektedir.

İnternetin gelişmesi ve çevrimiçi ortamlara kolay erişim, beraberinde hükümetlerin siber güvenliği koruması için uluslararası işbirliklerini sağlaması ve bu konuda çalışmaların yapılması önerilmektedir. Bunun yanı sıra akademik yayın önerileri olarak

üretken yapay zeka, blokzincir vb. yeniliklerinin kullanılarak siber güvenlik uygulamalarının farkındalığını artırmaya yönelik çalışmaların yapılması da önerilmektedir.

Kaynakça

Alghazo, J. M., Kazmi, Z. & Latif, G. (2017). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. *2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)* (1-6). IEEE.

Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A. & Islam, S. (2022). Cyber security threats on digital banking. *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (1-4). IEEE.

Asmar, M. & Tuqan, A. (2024). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon, 10*(17).

Ateş, A., Kurt, A. & Sunar, H. (2024). Bibliometric analysis of studies on Google Maps. *Selcuk Tourism and Information Research Journal, 5*, 36-51.

Atkins, L., Banerjee, S., Boer, M., Craig, L., Greis, J., Hao, G. & Idler, M. (2024). The cyber clock is ticking: Derisking emerging technologies in financial services. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services. Erişim Tarihi: 29.10.2024.

Babu, B. B. (2018). Cyber security in banks. https://www.iibf.org.in/documents/BankQuest/Bank-Quest-Jan-Mar-2018-Final-200418.pdf. Erişim Tarihi: 29.10.2024.

Birindelli, G. & Iannuzzi, A. P. (2024). The systemic importance of cyber risk in banks. *Systemic risk and complex networks in modern financial systems* (301-321). Cham: Springer Nature Switzerland.

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.

Bozkus Kahyaoglu, S. & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360-376.

Cele, N. N. & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, https://doi.org/10.1108/JFC-10-2023-0263

Ghelani, D., Hua, T. K. & Koduru, S. K. R. (2022). *Cyber security threats, vulnerabilities, and security solutions models in banking.* Authorea Preprints.

Guleria, D. & Kaur, G. (2021). VOSviewer ve RStudio Bibliometrix kullanılarak eko-girişimciliğin bibliyometrik analizi, 1989–2019, *Library Hi Tech, 39*(4), 1001-1024. https://doi.org/10.1108/LHT-09-2020-0218

Haksever, B. F. & Baykal, B. (2023). Bankacılık sektöründe dijitalleşme ve finansal teknolojilerin hizmet pazarlamasına etkileri. *Akademik Açı*, *3*(2), 191-228.

Hanif, Y. & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust. *Technology in Society*, *67*, 101693.

Harvey, J. & Lau, S. F. (2009). Crime-money, reputation and reporting. *Crime, Law and Social Change*, *52*, 57- 72.

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M. & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), 41-59.

Huang, Y., He, X., Lian, Z. & Yang, Z. (2024). Mapping the landscape of digital cultural heritage research: A quantitative and visual bibliometric study. https://doi.org/10.1108/LHT-09-2023-0465

International Monetary Fund (IMF). Monetary and Capital Markets Department. (2024). Cyber Risk: A Growing Concern for Macrofinancial Stability. *Global Financial Stability Report*, USA: International Monetary Fund. https://doi.org/10.5089/9798400257704.082.CH003

Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M. & Albanna, A. (2024). Online banking user authentication methods: A systematic literature review. *IEEE Access*.

Khan, H. U., Malik, M. Z., Nazir, S. & Khan, F. (2023). Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis. *IEEE Access*.

Korkmaz, Ö. F., Soğukoğlu Korkmaz, S. & Sunar, H. (2023). Kamu ve özel bankalarda mobil bankacılık özelliklerinin mobil bankacılık kalitesi üzerine ve mobil bankacılık kalitesinin banka itibarı üzerine etkisinin belirlenmesi: Giresun ili örneği. *Akşehir Meslek Yüksekokulu Sosyal Bilimler Dergisi*, *16*, 146-160.

Korkmaz, S. S. & Korkmaz, Ö. F. (2016). Sosyal medya ve türk bankacılık sektörünün sosyal medya kullanımı. *Giresun Üniversitesi İktisadi ve İdari Bilimler Dergisi*, *2*(3), 58-84.

Kumar, B. S. & Ravi, V. (2016). A survey of the applications of text mining in financial domain. *Knowledge-Based Systems, 114*, 128-147.

Kumar, M. (2023). An overview of cyber security in digital banking Sector. *East Asian Journal of Multidisciplinary Research*, *2*(1), 43-52.

Mahboob, S. M., Abbas, S. S. & Shaheen, I. A. (2023). Adapting to cybersecurity challenges: Assessıng the effectiveness of international law against cyber terrorism. *Journal of Social Research Development*, *4*(4), 669-685.

Mongeon, P. & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: a comparative analysis. *Scientometrics*, *106*, 213-228.

Nurjannah, S. (2023). Digital transformation in the banking industry challenges and opportunities. *International Journal of Accounting, Management and Economics*, *1*(01).

Oyewole, A. T., Okoye, C. C., Ofodile, O. C. & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643.

Qiao, G., Ding, L., Zhang, L. & Yan, H. (2021). Accessible tourism: A bibliometric review (2008-2020). *Tourism Review, 77*(3), 713-730.

Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J. & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, *60*, 101616.

Thach, N. N., Hanh, H. T., Huy, D. T. N. & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845.

Unit21. (2022). 24 neobank statistics to help with risk and compliance. https://www.unit21.ai/blog/neobank-statistics#statistics-about-neobank-market-size-and-share. Erişim Tarihi: 15.10.2024.

Varol, H. C. & İşler, D. B. (2024). Dijitalleşme sürecinde müşteri deneyiminin müşteri sadakati ilişkisi: Bankacılık sektöründe bir uygulama. *Uluslararası Global Turizm Araştırmaları Dergisi*, *8*(1), 1-20.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G. & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160.

Wang, V., Nnaji, H. & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415.

Çıkar Çatışması: Yoktur.

Finansal Destek: Yoktur.

Etik Onay: Yoktur.

Yazar Katkısı: Ömer Faruk KORKMAZ (%50), Selin SOĞUKOĞLU KORKMAZ (%50)

Conflict of Interest: None.

Funding: None.

Ethical Approval: None.

Author Contributions: Ömer Faruk KORKMAZ (50%), Selin SOĞUKOĞLU KORKMAZ (50%)

A Retrospective Qualitative Study: Banking and Cyber Security

Ömer Faruk KORKMAZ & Selin SOĞUKOĞLU KORKMAZ

Extended Abstract

The world today, which has evolved from an industrial society to an information society, is exposed to the effects of technology and innovation, which are the visible reflections of the knowledge acquired. While the size of lands or the number of factories were important in yesterday's world, in today's world, it is observed that elements such as the storage, processing, and transfer of information make a difference. Therefore, in order to stand out in the increasing competition and maintain this advantage, it is observed that businesses are intensively using information technologies, and during this process, sectors are digitalizing. Banks that serve a wide societal audience are inherently required to store and process a variety of valuable documents, papers, and information. Additionally, they also carry out many financial transactions. Therefore, the security of the entire system of these financial transactions must be ensured. It is also clear that the security of banks, which are considered the most fundamental institutions of the financial system in national economies, means the security of many economic stakeholders, from savers to investors, from financial intermediaries to governments. It seems possible that a potential cyber vulnerability could spread throughout the entire economy and cause widespread damage. While the importance of the trust mechanism in the healthy functioning of the banking sector is known, it is also known that digital banking is exposed to and will continue to be exposed to cyber risks. Therefore, all processes, policies, and practices related to cybersecurity in the sector are of great importance. In today's digital age, the banking sector is undergoing a significant transformation alongside technological advancements. Innovations such as internet banking, mobile applications, and digital payment systems have facilitated access to financial services. The latest reflection of financial technology in the banking sector is digital banking. With digital banking, various concerns regarding financial security are emerging. The importance of cybersecurity in the banking sector is based on the need to protect the assets and sensitive information of both financial institutions and customers.

This study aims to systematically evaluate the literature addressing the use of cybersecurity in the banking sector. In this context, the subject of the study is cybersecurity in banking. Therefore, literature studies related to the cybersecurity needs arising as a result of the increasing digital usage in the banking sector are being addressed. By examining academic studies in this field, bibliometric methods have been utilized to contribute to the literature and prevent the repetition of studies. In this context, a search was conducted in the Web of Science database using the terms "banking" and "cyber security." Only research articles were preferred, and in this context, the dataset consisted of 88 studies. In the analysis of these data and the visualization of relationship networks, the Bibliometrix and VOSviewer applications were utilized.

When the dataset created for bibliometric analysis was examined, it was found that the oldest study was conducted in 2011. This situation also indicates that the topic is a current issue. It is observed that the number of research articles between the years 2011 and 2020 is quite low. As of 2020, the acceleration of digitalization, the increase in mobile applications, and especially due to the COVID-19 pandemic, the development of internet-based mobile technologies and the mandatory use of contactless technologies have raised security-related issues. It is believed that this situation has contributed to the increase in the number of publications. In the reviewed research articles, there are a total of 169 authors. Approximately 34% of their articles consist of internationally co-authored works. The average number of authors per research article has been calculated to be approximately 3.42. These data indicate that there is a common international interest in the research topic. In the study, besides the search terms "cybersecurity" and "banking," other prominent keywords that emerged were fintech, internet banking, text mining, cyber attack, cyber risk, machine learning, phishing (fraud), and cyber resilience. In the examined studies, analyses were conducted on the prominent and high-impact research topics based on authors, keywords, citation statuses, countries, and bibliographies.

As a result of the study, it was determined that the number of publications increased after 2019, and keywords related to the concepts of fintech and cybersecurity were more frequently addressed. When examining the distribution of publications by country, the countries with the most publications on the subject were India, Pakistan, Jordan, the USA, and the UK, in that order. For the 88 research articles examined, machine learning and authentication themes were identified as the prominent niche themes. It is observed that interest in themes such as management, digital banking, risk, cybersecurity, awareness, banking, finance, internet services, threats, prediction, and COVID-19 continues. However, it has been observed that themes such as mobile applications, user experience, evaluation, and performance have lost their popularity in the studies.

Many of the studies conducted in the fields of artificial intelligence and digital transformation still face significant challenges in understanding the speed at which technology can advance and the potential outcomes. It is known that traditional banking has significant gains in the adoption of innovations brought by artificial intelligence and information technologies. However, this does not mean that traditional banks have access to all the advantages of digital banking. The high loyalty of customers to traditional banks, the low acceptance of technology usage, the impact of the average customer age on the preference for digital banking, and the presence of cybersecurity issues explain the slow transformation of banking. These factors can also be listed among the reasons for the weakness of digital banking. Many of these mentioned deficiencies seem to be surmountable through marketing and retention efforts. However, since cybersecurity is distinct from these in terms of its structure, the cybersecurity system needs to be as dynamic as the factors that can put it at risk and quickly adopt technological innovations.

A cyber threat can be defined as a malicious act where someone attempts to access digital banking without authorization and permission. Despite many preventive measures, it cannot be ensured against the security issues that have arisen with the digitization of banking. In banking, addressing these concerns and achieving a healthy improvement depend on various factors, such as the existence of an adopted risk assessment methodology, a well-developed robust cybersecurity culture, high cybersecurity awareness among employees and customers, and high compliance with regulatory requirements. Among the primary factors that reduce cybersecurity capability are the lack of advanced technology and inadequate legal compliance. To prevent cybersecurity breaches, banks should take on more responsibility for reducing cybersecurity risks. Because it is known that financial consumers access financial products and services from a wide variety of sources. Managing the threats coming from these access points can also be more difficult for them compared to corporate structures.

The high contagion risk in the financial sector also applies to cyber threats, which can permeate the entire financial system through systemic effects and,disrupt stability. Therefore, regulatory and supervisory authorities are trying to encourage the increase of cybersecurity levels and the strengthening of governance controls. Therefore, addressing cybersecurity breaches without falling into the mistake of treating them solely from a banking perspective and enhancing resilience and cooperation through international legal regulations is of paramount importance. The existence of current initiatives such as the emergence of cyber stress tests and standardized cyber risk protocols indicates progress in this direction. The increase in employees' ability to use digital systems in processes and systems transitioning from traditional to digital can be listed among the factors that could be effective at this point. Additionally, cybersecurity companies need to work closely with banks to stay ahead of cyber threats and take on a proactive role. Ultimately, the existence and implementation of digital strategic plans for digital banking can guide the banks of the future from today. Digital transformation essentially brings very significant gains. Opportunities for improving performance and consumer behavior can be given as examples of this. However, the necessity of changes in the corporate structure due to technological innovations also brings various challenges. Of course, for the finance sector, which has been using computer automation systems for more than a quarter of a century, cyber risk management is not a new phenomenon. However, a robust and comprehensive cyber risk management strategy has never been more critical. Moreover, regulatory and supervisory authorities, cybersecurity companies, and financial sector organizations should improve their employee capabilities and ecosystems against cyber breaches, in addition to using advanced technology. It will be important for financial institutions to keep their environment ready for cybersecurity from today. Moreover, as financial sector institutions expand their digital footprints, this importance seems to be increasing. It is known that security is a response to risk. Therefore, the issue of cybersecurity should be addressed proactively. In addition while financial sector organizations willingly adopt advanced technology products, they must take action now to address the increasing cyber risks. This action should be taken to prepare the environment for the future. It should not be forgotten that today's trending technologies can change and become obsolete for tomorrow.