NEU PRESS

JGEHES Journal of General Health Sciences
GENEL SAĞLIK BİLİMLERİ DERGİSİ

Cilt/Volume:6 Sayı/Issue:3 Yıl:2024 Araştırma Makalesi/Research Article e-ISSN: 2687-5403

https://doi.org/10.51123/jgehes.2024.139

# Sağlıkta Bilgi Güvenliği Yönetiminin Bibliyometrik Analizi

**Yusuf Yalçın İLERİ[1] Muhammed Yusuf AYDAMAK[1]**

[1]Necmettin Erbakan Üniversitesi, Nezahat Keleşoğlu Sağlık Bilimleri Fakültesi, Sağlık Yönetimi Bölümü, Türkiye

**Makale Bilgisi**

**Makale Geçmişi**

**Geliş Tarihi:** 09.06.2023
**Kabul Tarihi:** 03.10.2023
**Yayın Tarihi:** 25.12.2024

**Anahtar Kelimeler**
Bilgi Sistemleri,
Bilgisayar Güvenliği,
Sağlık Bilgi Sistemleri,
Gizlilik,
Tıbbi Bilişim.

**ÖZET**

Çalışmada sağlık kurumlarında bilgi güvenliği yönetimi konusunda yapılan akademik çalışmaların incelenmesi ve değerlendirilmesi amaçlanmaktadır. Bu açıdan çalışmada sağlık kurumlarında bilgi güvenliği yönetimi alanında en fazla atıf ve yayını olan dergiler, yayınlar, yazarlar ve kurumlar, alandaki eş yazarlık ve anahtar kelimelerin eş birliktelikleri ile birlikte dönemsel değişimleri araştırılmıştır. Bu amaç doğrultusunda bibliyometrik bir çalışma yapılmıştır. Web of Science veri tabanında 1982-2023 aralığında yapılan yayınlar VOSviewer programı kullanılarak analiz edilmiştir. Araştırma performans analizleri (dergiler, ülkeler, yayınlar, atıflar vb.) ve bibliyometrik analizler (eş yazarlık, anahtar kelimeler eş birliktelik ve dönem dağılımı) olarak iki boyut altında yürütülmüşür. Çalışmada elde edilen verilerin analiz sonucunda alanda yayın ve atıf sayılarının son dönemde yoğunlaştığı tespit edilmiştir. Yayın ve atıf sayısı açısından ABD öncü pozisyondadır. Alanda atıf/yayın sayısı etkililiğinde IEEE'nin öne çıktığı; en fazla yayının De Montfort Üniversitesi'nce yapıldığı; en fazla atıfın Hong Kong Üniversitesi ve Salerno Üniversitesi'nde olduğu ve alanın en etkili yazarının Christian Esposito olduğu görülmüştür. Çalışmada sonuç olarak bilgi güvenliği konusunun hukuki, etik ve örgütsel (personel algısı, dijital okuryazarlık vb.) perspektiflerini ele alan çalışmaların yapılmasının alana katkı sağlayacağı değerlendirilmektedir.

## Bibliometric Analysis of Information Security Management in Healthcare

**Article Info**

**Article History**

**Received:** 09.06.2023
**Accepted:** 03.10.2023
**Published:** 25.12.2024

**Keywords**
Information Systems,
Computer Security,
Health Information Systems,
Confidentiality,
Medical Informatics.

**ABSTRACT**

The study aims to assess academic researches on information security management in healthcare organizations along with their temporal trends on spesific topics, such as top-cited journals, publications or authors. We conducted a bibliometric analysis for this purpose. We analyzed publications in the Web of Science database spanning 1982-2023 via VOSviewer program. The research comprised two dimensions: performance analyses, which considered metrics such as the (journals, countries, publications, citations) and bibliometric analyses, which encompassed (co-authorship, keywords co-occurrence and their temporal period distribution).The analysis revealed a recent upwing in both the number of publications and citations within the field. The USA emerged as a fronrunner in term of both publications quantity and citations count. Notably, IEEE demonstrated notable effectiveness in ratio of citations to publications. De Montfort University stood out as the institution with the highest number of publications, while the most frequently cited contributions originated from Hong Kong University and Salerno University. Additionally, Christian Esposito emerged as the most influential author in the field based on citation metrics. In light of the study's findings, it is evident that the field of information security management in healthcare organiations is experiencing growth. To further enhance this domain, it is recommended that future research endeavors focus on addressing multifaceted aspects such as legal, ethical and organizational considerations, which include personnel perception and digital literacy. These inclusive studies are likely to make substantial contributions to the field, fostering a more comprehensive understanding o information security in healthcare organizations.

**To cite this article**

İleri, Y.Y. & Aydamak, M., Y. (2024). Sağlıkta bilgi güvenliği yönetiminin bibliyometrik analizi. *Genel Sağlık Bilimleri Dergisi*, *6*(3), 409-432. https://doi.org/10.51123/jgehes.2024.139

***Sorumlu Yazar:** Muhammed Yusuf AYDAMAK, muhammedaydamak@gmail.com

## GİRİŞ

Sağlık hizmetleri bilgiye dayalı olarak ilerleyen bir hizmet alanıdır (Altındiş, 2012). Sağlık hizmetlerinde bilgi ifadesi hastanın hekimine açık ve anlaşılır bilgiye dayalı anemnez vermesinden elektronik sağlık kayıtları gibi bilgi teknolojilerinin gelişmesine kadar geniş bir perspektifi kapsamaktadır (Peikari ve ark., 2018). Bu noktada sağlık hizmetlerinin temel uğraş alanının "insan ve insan hayatı" olması göz önüne alındığında hizmetin sıfır hata ilkesinde sunulması gereklidir (Varol ve ark., 2016). Sıfır hatanın sağlanması ise ancak doğru ve tam bilgiye dayalı olarak gerçekleşmektedir (Koppel, 2012). Sağlık kurumlarının sıfır hata hedefine yaklaştıran bir hizmet sunabilmesi başta hasta verileri olmak üzere sahip oldukları sağlık bilgisinin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamalarına bağlıdır (Sari ve ark., 2022). Bu üç bağlamın herhangi birinde yaşanacak bir aksaklık sonucu açığa çıkacak olan sağlık bilgisinin amaç dışı kullanılma potansiyeli bulunmaktadır (Yeng ve ark., 2022). Bu bakımdan sağlık kurumları sağlık bilgisini korunabilir kılacak güvenilir bir bilgi güvenliği yönetimi sistemini teşkil etmek zorunda kalmaktadır (Esposito ve ark., 2018). Ayrıca bilişim sistemlerinin yaygınlaşması vasıtasıyla her türlü sağlık bilgisinin elektronik olarak kaydedilme imkânı doğması ve bunun sonucunda sağlık kurumlarındaki sağlık bilgilerinin büyük hacimlere kavuşması bilgi güvenliği yönetimini kaçınılmaz kılmaktadır (İleri, 2018).

Sağlık kurumları sahip oldukları bilgi yönetim sistemleri açısından karmaşık bir yapıdadır. Bu durumun doğal bir sonucu olarak sağlık kurumlarındaki bilgi güvenliği yönetimi de kompleks bir yapı niteliğini taşımaktadır (Karaarslan ve ark., 2015). Bu sistemler münferit bir sistem olmayıp birbiri ile entegre farklı sistemler ile birlikte çalışabilen sistemler bütünüdür (İleri, 2018). Bu kompleks yapıda etkin bir güvenlik için sağlık kurumlarının gerçekleştireceği ilk eylem iyi hazırlanmış bir politika çerçevesi olmalıdır (Moody ve ark., 2018). Aynı zamanda karmaşık bilgi sistemleri ortamında bireylerin iyi bir teknoloji okuryazarlığına sahip olması da önemlidir (Kılcan ve Gülbudak, 2019). Bu noktada sürecin işleyişine bakıldığında bilgi sistemleri aracılığıyla sağlık bilgisi hekimler, sigorta kuruluşu veya kamu kurumları gibi farklı kullanıcılar arasında sürekli olarak karşılıklı değişim ve müdahale içerisinde olmaktadır (Li ve ark., 2010). Farklı kullanıcıların sisteme bu şekilde dahil olmasında sağlık kurumları bilgi güvenliğini yetkilendirme yaparak sağlayabilmektedir. Sisteme dahil olacak her kullanıcıya yetkisi bazında erişim alanı açılması kullanıcının yalnızca erişmesi gereken bilgilere erişmesini sağlayacaktır. Bu durum bilgi güvenliğini geçerli kılacaktır (Lundgren ve Möller, 2019).

Sağlık kurumları için bir başka önemli nokta kesintisiz bir iş akışı süreci sürdürmelerinin gerekliliğidir. Sağlık hizmetinin bilgiye dayalı olmasından dolayı bilgi akışı ve güvenliğinde yaşanacak olası bir aksaklık hizmet sunumunu durdurma potansiyelini taşımaktadır (Yeng ve ark., 2022). Örneğin, 2020'de Almanya'da Düsseldorf Üniversitesi Hastanesi'ndeki ölümle sonuçlanan bilgi güvenliği ihlali olayı bu potansiyeli açık olarak ortaya koymaktadır (Silomon, 2020). İhlalin başladığı 10 Eylül 2020'de ve devamındaki hastane açıklamalarında hastane bilgi sistemlerine siber saldırı yapıldığı ve saldırıdan dolayı bilgi sistemlerinin tamamen çöktüğü ifade edilmektedir. Bu çöküntüden dolayı hastane hiçbir şekilde sağlık hizmeti veremediğini açıklamıştır. Ayrıca, hastanenin bulunduğu Kuzey Ren Vestfalya Eyaleti'nin acil servis sistemi ile de iletişiminin aksadığı ve bu durumdan dolayı hastanenin acil servisinin kapandığı ifade edilmiştir (Universitätsklinikum Düsseldorf, 2020a, 2020b, 2020c, 2020d, 2020e, 2020f, 2020g). Durum bu şekildeyken acil bir hastanın ambulans ile Düsseldorf Üniversitesi Hastanesi'ne doğru yolda olduğu durumu ortaya çıkar ancak hastane tıbbi görüntüleme sistemine erişim olmadığı gerekçesi ile hastayı daha hastaneye gelmeden kabul etmemiştir (Silomon, 2020). Bunun üzerine ambulans 30 km uzaklıktaki başka bir hastaneye sevk edilmek zorunda kalmış ancak hasta o hastaneye varamadan hayatını kaybetmiştir (Tidy, 2020). Eyalet resmi makamları ve Federal Bilgi Güvenliği

Ofisi bu ölümün siber saldırı nedeniyle gerçekleştiğini ifade ederek iki olay arasında doğrudan ilişki olduğunu kabul etmiştir (Bundesamt für Sicherheit in der Informationstechnik, 2020; SPIEGEL Netzwelt, 2020). Bu bağlamda sağlık bilgisinin doğal bir niteliği olarak sağlık kurumları oldukça hassas veri ve bilgi ile çalışmaktadır (Deniz, 2023). Bu hassas verilerin güvenliğinin sağlanması ve kesintisiz iş akışının sürdürülmesi sağlık kurumlarının uygulayacağı bilgi güvenliği yönetim sisteminin temel amaçları olmalıdır (Abouelmehdi ve ark., 2018).

Sağlıkta bilgi güvenliğinin sağlanması oldukça önemli ve hassas bir alan olmaktadır. Sağlık çalışanları ile bilgi güvenliği konusunda yapılan bir çalışmada sağlık çalışanlarının bilgi güvenliği için yeterince özen göstermeye çalıştığı ancak yeterli düzeyde sağlayamadıkları sonucuna ulaşılmıştır (Baran ve Şener, 2019). Bir diğer çalışmada ise sağlık çalışanlarının lisans düzeyinde öğrenim alırken bilgi gizliliği farkındalıklarının gelişmeye başladığına önem atfedilmektedir (Bahar ve ark., 2022). Birleşik Krallık Hükümeti Sağlık ve Sosyal Bakım Departmanı tarafından yayımlanan bir raporda 2017'de gerçekleşen ve ana hedefi Ulusal Sağlık Sistemi olmamasına rağmen sağlık sistemini etkileyen WannaCry siber saldırısının ardından bilgi sistemlerini iyileştirme maliyetlerinin 21 milyon sterlin ile başladığı ifade edilmektedir (Smart, 2018). Kişisel Verileri Koruma Kurumu tarafından yapılan bir duyuruda ise Türkiye'deki özel bir tıp merkezinde Şubat 2023'te bilgi güvenliği ihlali yaşandığı ve ihlal sonucunda yaklaşık 5 000 kişiye ait sağlık verilerinin etkilendiği ifade edilmektedir (Kişisel Verileri Koruma Kurumu, t.y.). Bunun yanı sıra kaçırılmaması gereken bir nokta olarak sağlık bilgisinin güvenilir olması sağlık profesyonellerinin mesleki bilgilerini doğru şekilde sunabilmeleri için önemlidir. Kulak burun boğaz uzmanı hekimler ile yapılan bir çalışmada hekimlerin mesleki eğitim için geliştirilecek eğitim modellerinde öncelikle bilgi kaynağının yani bilginin güvenilir olup olmadığına dikkat edilmesine önem atfetmişlerdir (Ture ve ark., 2022). Bu açıdan bakıldığında sağlık kurumlarında yaşanacak olası bilgi güvenliği ihlalleri mali sonuçlardan, veri kaybına ve hatta hasta ölümüne yol açabilecek kadar ciddi sonuçlar doğurmaktadır. Bu durumdan dolayı sağlık kurumlarında bilgi güvenliğini ele alan çalışmalar yapılmasının önemli olduğu düşünülmektedir.

Bibliyometrik araştırmalar, ilgili çalışma alanına dair literatürdeki güncel durumu betimleyerek araştırmacıların alana dair önceden bir izlenim elde etmelerine imkân veren bir araştırma sistematiği sunar (Zupic ve Čater, 2015). Bibliyometri kavramı "Belirli bir alanda belirli bir dönemde ve belirli bir bölgede kişiler ya da kurumlar tarafından üretilmiş yayınların ve bu yayınlar arasındaki ilişkilerin sayısal olarak analizidir." şeklinde ifade edilmektedir (Cahit Arf Bilgi Merkezi, t.y.). Bu açıdan yapılan tanımda da ifade edildiği üzere bibliyometrik araştırmalar hâlihazırdaki mevcut akademik çalışmaları niceliksel olarak inceleyerek literatürdeki ilişki ağını ortaya çıkarmaktadır. Bibliyometrik araştırmalar ilişki ağlarının ortaya çıkarılmasında atıf, ortak atıf (co-citation), ortak kelime (co-word) veya bibliyometrik eşleştirme gibi çeşitli analizlerle çalışmaktadır (Hou ve ark., 2015; Polat ve ark., 2019). Bibliyometrik araştırmalar ilişki ağları ile birlikte alanda önde gelen başlıca aktörleri belirleyerek yeni araştırmacılar için bilimsel bir temel oluşturmaktadır (Martínez ve ark, 2015). Bibliyometrik çalışmalar "performans analizi" ve "bilimsel haritalama" olmak üzere iki kategoride yürütülmektedir. Performans analizi yayın veya atıf sayısı gibi göstergeleri ölçerek araştırmacılar tarafından alana yapılan katkıyı tanımlamaktadır. Bilimsel haritalamada ise ifade edilen ilişki ağı ortak yazarlık gibi çeşitli analiz türleri ile görsel olarak ortaya çıkarılmaktadır (Donthu ve ark., 2021).

Bu araştırmada ise sağlık kurumları için bu kadar önem arz eden bilgi güvenliği konusunda alanda çalışma yapacak araştırmacılar için bilimsel bir temel hazırlanması kaygısıyla bibliyometrik çalışma yapılmıştır. Yapılan incelemede bu konuda daha önce herhangi bir bibliyometrik çalışma yapılmamış olmasından ve bu çalışmanın bir ilk olacağından dolayı alandaki akademik birikim için önem arz edeceği varsayılmaktadır. Bu bağlamda çalışmada "sağlık kurumlarında bilgi güvenliği

yönetimi" konusundaki mevcut literatürün değerlendirilmesi, temel ilişki ağlarının ne olduğu ve hangi noktalarda çalışmalar yapıldığının belirlenmesi ve böylelikle alanda çalışma yapacak araştırmacılar için bilimsel bir temel hazırlanması amaçlanmaktadır. Bu amaç doğrultusunda çalışma bibliyometrik bir araştırma olacak şekilde tasarlanmıştır ve alana dair bilimsel haritalama ile birlikte tanımlayıcı nitelikte performans analizleri yapılarak betimsel çerçeve çizilmiştir. Bu bakımdan araştırma betimsel bir araştırmadır.

Araştırma ulaşılmak istenen araştırma soruları şu şekilde olmaktadır:

1. Sağlık kurumlarında bilgi güvenliği yönetimi alanında en fazla atıf alan dergiler, yayınlar ve yazarlar nasıl oluşmaktadır?

2. Sağlık kurumlarında bilgi güvenliği yönetimi alanında en fazla yayın yapan dergiler, ülkeler, kurumlar ve yazarlar nasıl oluşmaktadır?

3. Sağlık kurumlarında bilgi güvenliği yönetimi alanında anahtar kelimelerin eş birliktelikleri ve dönemsel kullanımları nasıl oluşmaktadır?

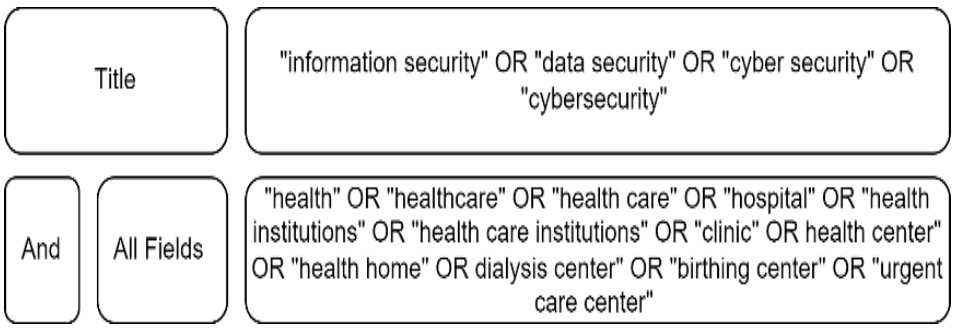
4. Eş yazarlık analizi doğrultusunda sağlık kurumlarında bilgi güvenliği yönetimi alanında ülkelerin, kurumların ve yazarların eş yazarlıkları nasıl oluşmaktadır?

## YÖNTEM

Bibliyometrik çalışmalarda genel olarak Web of Science (WoS), Scopus ve PubMed veri tabanları ile çalışılmaktadır (Chen, 2017). Bu yaygın veri tabanları arasında WoS'un daha standardize ve detaylı bilgi sağladığı belirtilmektedir (Hou ve ark., 2015). Ayrıca bu veri tabanları arasında en eski veri tabanı WoS'dur (Martín-Martín, 2021). WoS'un bu şekilde geriye dönük olarak standart ve detaylı bilgi sağlamasından dolayı dünyanın en önde gelen veri tabanı olduğu ifade edilmektedir (Martínez ve ark., 2015). Bu noktalar açısından mevcut araştırmada WoS inceleme veri tabanı olarak seçilmiştir. Araştırmada yayın taraması 28.5.2023 tarihinde WoS Core Collection'da yapılmıştır. Veri taramasında ilk olarak başlık araması seçilerek "information security", "data security", "cyber security" ve "cybersecurity" anahtar kelimeleri girilmiştir. Ardından ikinci bir arama sekmesi eklenmiş ve tüm alanlar araması seçilerek "health", "healthcare", "health care", "hospital", "health institutions", "health care institutions", "clinic", "health center", "health home", "dialysis center", "birthing center" ve "urgent care center" anahtar kelimeleri ile arama yapılmıştır. İkinci arama sekmesi eklenirken "ve" (and) bağlacı kullanılmıştır.

**Şekil 1**

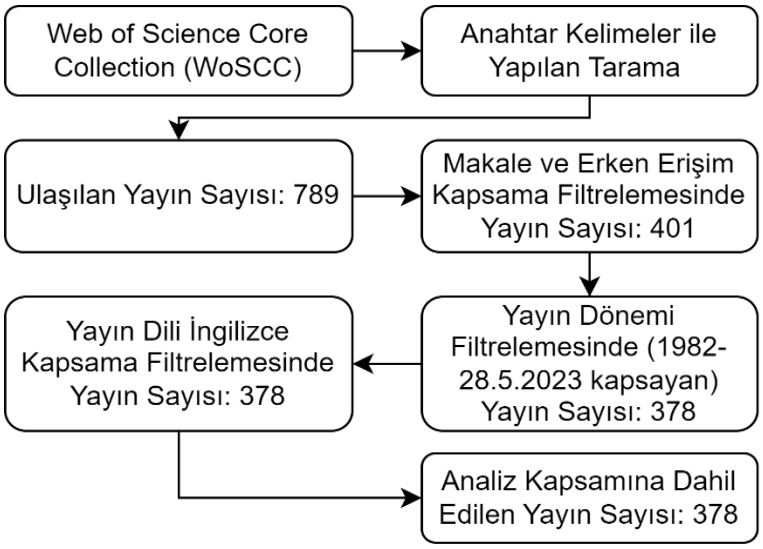
*WoS Core Collection'da Yapılan Tarama Yöntemi*



Bu anahtar kelimeler ile yapılan tarama ve uygulanan sınırlamalar doğrultusunda çalışma toplam 378 araştırma ile gerçekleştirilmiştir. Uygulanan sınırlama sınırlılıklar başlığı altında açıklanmıştır. Yürütülen süreç Şekil 2'de görsel olarak ifade edilmektedir.

**Şekil 2**

*Araştırma Tasarımı İş Akışı*




Çalışma açık kaynak üzerinden açık veriler ile yapıldığı için herhangi bir etik izne ihtiyaç duyulmamıştır. Araştırma analizlerinde ayrıca VOSviewer programının 1.6.16 sürümünden faydalanılmıştır. VOSviewer, bibliyometrik haritalama yapılması ve verilerin görselleştirilmesi amacıyla kullanılan bir programdır (Van Eck ve Waltman, 2010).

## BULGULAR

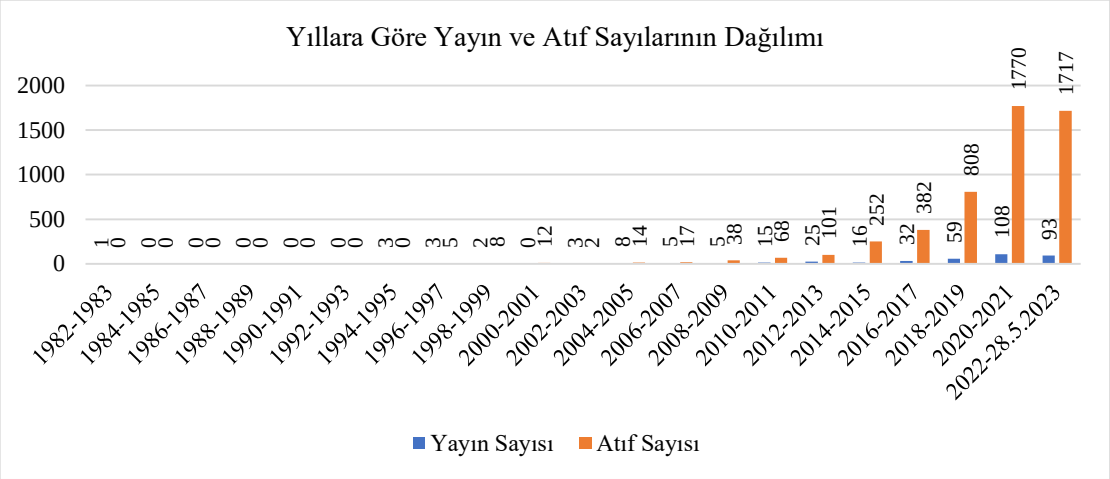
Yapılan bibliyometrik analizler sonucunda elde edilen bulgular bu bölümde başlıklar halinde ifade edilmektedir. Analizler temel olarak VOSviewer programı ile gerçekleştirilmiştir ancak bununla birlikte bazı analizlerde WoS'un sunduğu veriler kullanılmıştır.

### Performans Analizleri

İfade edildiği üzere araştırma 378 yayın ile gerçekleştirilmiştir. Bu bakımdan araştırma kapsamındaki yayınların dağılımları dönemlerine göre olmak üzere atıf sayıları ile birlikte Grafik 1'de gösterilmektedir.

**Grafik 1**

*Yıllara Göre Yayın ve Atıf Sayılarının Dağılımı*




Grafik 1 WoS verilerine dayalı olarak oluşturulmuştur. Buna göre 1982-1983 olan ilk yayın döneminin akabinde uzun bir dönem yayın sayısında herhangi bir artış görülmemektedir. Atıf sayıları içinde benzer bir durum söz konusudur. İlk atıf 1996-1997 döneminde gelmiştir. Ancak artış trendinin 2008-2009 döneminde başladığı ve son dört yıllık dönemde pik yaptığı görülmektedir. Bununla birlikte yayın sayılarında son dönemde artış yaşanmış olsa da atıf artış oranına göre oldukça düşük kalmıştır. Grafik 1'e göre toplam atıf sayısı 5. 194'tür. Atıf sayısının yılbaşına ortalaması ise 123.66'dır. Ancak hem atıf hem de yayın sayısında yoğunlaşma 2018-28.5.2023 aralığındaki son altı yıllık dönemdedir. Bu dönem aralığı toplam atıf sayısının %82.69'unu (n=4.295) ve toplam yayın sayısının %69.78'ini (n=260) oluşturmaktadır. Bu durum dolayısıyla bu dönem aralığına dair bir oranlama yapıldığında son altı yılın atıf ortalaması 1 369 olurken yayın ortalaması 74'tür. Atıf değerlendirmesinde diğer bir nokta kendine atıflarda görülmektedir. WoS Atıf Raporu'na göre toplam atıf sayısı içinde kendine atıf sayısı %3.25 (n=169)'dir. Bu açıdan kendine atıf oranının düşük olmasının alan için olumlu bir gösterge olduğu değerlendirilebilir. Tablo 1'de ise en çok yayın yapılan akademik kaynaklara yer verilmektedir. VOSviewer programı ile oluşturulan bu sınıflandırmada ilk ona giren dergiler arasında on beş yayın sayısı ile en çok yayın yapılan derginin "Computers & Security" olduğu görülmektedir.

**Tablo 1**

*En Fazla Yayın Yapılan İlk 10 Dergi.*

| Sıra | Kaynak Adı | Yayın Sayısı | Atıf Sayısı | Yayımcı |
|---|---|---|---|---|
| 1 | Computers & Security | 15 | 380 | Elsevier |
| 2 | International Journal of Medical Informatics | 10 | 199 | Elsevier |
| 3 | Applied Science-Basel | 10 | 84 | MDPI |
| 4 | Healthcare | 7 | 34 | MDPI |
| 5 | IEEE Access | 7 | 117 | IEEE |
| 6 | IEEE Transactions on Industrial Informatics | 5 | 57 | IEEE |
| 7 | Journal of Medical Internet Research | 4 | 91 | JMIR Publications |
| 8 | Energies | 4 | 85 | MDPI |
| 9 | Health Information Management Journal | 4 | 63 | SAGE Publicatios |
| 10 | Intelligent Automation and Soft Computing | 4 | 19 | SAGE Publications |

En fazla yayın yapan bu ilk on dergi alandaki toplam yayın sayısının %18.51'ini (n=70) oluşturmaktadır. İlk üç derginin ise ilk onun %50'sini (n=35) oluşturduğu görülmektedir. Derlenen dergiler WoS Journal Citation Report (JCR) sınıflandırmasına göre kategorik olarak incelendiğinde yapılan yayınların genel olarak sağlık bilişimi ve bilgisayar bilimi-bilgi sistemleri kategorilerinde yer aldığı görülmektedir. Nitekim ilk iki dergi doğrudan bu kategorilerin içerisinde yer almaktadır. "Healthcare" dergisi için ise JCR bilgisine ulaşılamamıştır. Ancak en fazla yayın yapılan dergiler atıf sayıları açısından incelendiğinde ilk on sıralamasında değişkenlik yaşandığı görülmektedir.

**Tablo 2**

*En Fazla Atıf Alan İlk 10 Dergi.*

| Sıra | Kaynak Adı | Atıf Sayısı | Yayın Sayısı | Yayımcı |
|---|---|---|---|---|
| 1 | Computers & Security | 380 | 15 | Elsevier |
| 2 | IEEE Cloud Computing | 360 | 1 | IEEE |
| 3 | IEEE Wireless Communications | 317 | 1 | IEEE |
| 4 | International Journal of Medical Informatics | 199 | 10 | Elsevier |
| 5 | MIS Quarterly | 195 | 2 | MIS Reserach Center, Minnesota |
| 6 | Transport Reviews | 177 | 1 | Taylor & Francis Ltd. |
| 7 | Health Informatics Journal | 160 | 3 | SAGE Publications |
| 8 | JMIR mHealth and uHealth | 133 | 1 | KMIR Publications |
| 9 | IEEE Access | 117 | 7 | IEEE |
| 10 | Computer Communications | 111 | 2 | Elsevier |

Atıf sayıları incelendiğinde Tablo 1'deki dergilerden yalnızca üçünün sıralamaya girebildiği görülmektedir. Alanda en fazla yayını olan "Computers & Security'nin aynı zamanda en fazla atıf sayısına da sahip olduğu görülmektedir. En fazla yayını olan ikinci dergi ise atıf sayıları içerisinde dördüncü sırada yer almıştır. Tablo 1 ve Tablo 2'deki veriler görece olarak birlikte yorumlandığında "IEEE" ve "Elsevier" yayımcı olarak alanda öncü pozisyonda gözükmektedir. Ancak IEEE'nin bu rekabette önde olduğu değerlendirilebilir. Nitekim IEEE'nin iki farklı dergisinin yalnızca bir yayını olmasına rağmen aldığı atıf açısından ikinci ve üçüncü sırada yer almaktadır.

Bu durum etki oranı açısından da görülmektedir. IEEE dört dergisi ile 60.78 etki oranına sahipken Elsevier üç dergisiyle 25.55 etki oranına sahiptir. Oransal olarak IEEE'nin ileride olduğu açıkça ortadadır. Bu noktada Elsevier ile aynı sayıda toplam üç dergisi olan "SAGE Publications" değerlendirilirse etki oranı 22 çıkmaktadır Elsevier'e oldukça yakın gözükmektedir. Ancak SAGE Publications'u bu noktaya yalnızca bir dergisi taşımaktadır. "Health Informatics Journal"ın atıf sayısında gösterdiği performans etkili olmuştur. Ancak bu dergi en fazla yayın sıralamasında liste dışı kalmıştır.

İki listede de birinci olması açısından Computers & Security dergisinde genel olarak hangi konuların çalışıldığının tespit edilmesiyle amacıyla yayınlanan on beş makalenin özetleri incelenmiştir. İnceleme sonucunda bu dergide çalışılan konuların ulusal ve kurumsal düzeyde bilgi güvenliği politikaları (n=5), davranış bilimleri ve bilgi güvenliği ilişkisi (n=3), risk analizi (n= 2), ihlal analizi (n=1), hemşirelik öğrencileri ve bilgi güvenliği farkındalığı (n=1), nüfusta bilgi güvenliği okuryazarlığı (n=1), Covid-19 pandemisi ve alanyazına etkisi (n=1) ve bilgi güvenliğinde bilişsel ve kültürel önyargılar (n=1) olduğu tespit edilmiştir. Computers & Security haricindeki diğer iki Elsevier dergisinde çalışılan konu başlıkları ise bilgi güvenliği politikası ve sistem tasarımı (n=4), risk analizi (n=2), bilgi güvenliği ve sağlık sistemlerinde birlikte çalışabilirlik (n=1), bilgi güvenliği değerlendirmesi (n=1), bilgi güvenliği farkındalığı, beklentileri ve etik kaygılar (n=1), ihlal nedenlerine dair kök-neden analizi (n=1), örnek durum incelemesi (n=1) ve bilgi güvenliği mühendisliğidir (n=2). Bu analiz IEEE dergileri için yapıldığında çalışılan konu başlıklarının bilgi güvenliği mühendisliği ve veri analizi (n=8), bilgi

güvenliği yönetimi (yönetim boyutu) (n=2), ihlal nedenlerine dair kök-neden analizi (n=1), risk tanımlaması (n=1), risk analizi ve önceliklendirme (n=1) ve siber güvenlik olgunluk değerlendirmesinden (n=1) oluştuğu tespit edilmiştir. VOSviewer'den elde edilen verilere göre hazırlanan Tablo 3'te en fazla yayına sahip ülkelere atıf sayıları ile birlikte yer verilmektedir.

**Tablo 3**

*En Fazla Yayın Yapılan İlk 10 Ülke.*

| Sıra | Ülke | Yayın Sayısı | Atıf Sayısı |
|---|---|---|---|
| 1 | Amerika Birleşik Devletleri | 105 | 2384 |
| 2 | Hindistan | 55 | 511 |
| 3 | Çin Halk Cumhuriyeti | 40 | 868 |
| 4 | İngiltere | 31 | 443 |
| 5 | Suudi Arabistan | 29 | 194 |
| 6 | Avustralya | 21 | 211 |
| 7 | Malezya | 12 | 96 |
| 8 | İtalya | 11 | 410 |
| 9 | Tayvan | 11 | 159 |
| 10 | Pakistan | 11 | 93 |

Amerika Birleşik Devletleri (ABD) hem yayın hem de atıf sayısı olarak açık bir şekilde ilk sırada yer almaktadır. Tabloda ABD'nin ardından yayın sayısı olarak Hindistan gelirken atıf sayısı açısından Çin Halk Cumhuriyeti (ÇHC) gelmektedir. Tabloda Malezya ve Pakistan dikkat çekmektedir. Yayın sayısı açısından ilk on içerisine girmelerine rağmen atıf sayılarında diğer ilk on ülkelere göre oransal olarak geri planda kalmışlardır.

**Tablo 4**

*En Fazla Atıf Alan İlk 10 Ülke.*

| Sıra | Ülke | Atıf Sayısı | Yayın Sayısı |
|---|---|---|---|
| 1 | Amerika Birleşik Devletleri | 2384 | 105 |
| 2 | Çin Halk Cumhuriyeti | 868 | 40 |
| 3 | Hindistan | 511 | 55 |
| 4 | İngiltere | 443 | 31 |
| 5 | İtalya | 410 | 11 |
| 6 | Almanya | 364 | 10 |
| 7 | Singapur | 255 | 4 |
| 8 | Avustralya | 211 | 21 |
| 9 | Finlandiya | 204 | 4 |
| 10 | Suudi Arabistan | 194 | 29 |

Ülke değerlendirmesine atıf sayısı açısından bakıldığında nispeten ciddi bir değişikliğin olmadığı görülmektedir. En fazla yayına sahip ilk on ülkeden yedisi sıralamada kalmayı başarmıştır. Nitekim Hindistan ve ÇHC'nin yer değiştirmesi haricinde ilk dördün aynı kaldığı değerlendirilebilir. Bu tabloda özellikle Singapur ve Finlandiya dikkat çekmektedir. Yalnızca dört yayına sahiptirler ve diğer ülkelere göre bu rakam oldukça düşük gözükmektedir. Ancak buna rağmen atıf sayısı açısından oldukça etkin pozisyondadırlar. Türkiye ise 86 atıf sayısı ile atıf sıralamasında on dokuzuncu sıradadır. WoS Funding Agencies verileri derlenerek hazırlanan Tablo 5'te akademik çalışmalara en fazla finansal kaynak sağlayan ilk on kuruma yer verilmektedir.

**Tablo 5**
*En Fazla Finansal Destek Sağlayan İlk 10 Kurum.*

| Sıra | Finansman Sağlayan Kurum | Yayın Sayısı |
|---|---|---|
| 1 | Çin Ulusal Doğa Bilimleri Vakfı | 10 |
| 2 | Avrupa Komisyonu | 9 |
| 3 | ABD Ulusal Bilim Vakfı | 6 |
| 4 | ABD Sağlık ve İnsan Hizmetleri Bakanlığı | 6 |
| 5 | ABD Ulusal Sağlık Enstitüleri | 5 |
| 6 | Mühendislik ve Fizik Bilimleri Araştırma Konseyi – İngiltere | 4 |
| 7 | Birleşik Krallık Araştırma ve İnovasyon | 4 |
| 8 | Bilimsel ve Teknolojik Gelişim Ulusal Konseyi - Brezilya | 3 |
| 9 | ÇHC Guangdong Eyaleti Ulusal Doğa Bilimleri Vakfı | 3 |
| 10 | Kore Ulusal Araştırma Vakfı | 3 |

Tablo 5'e göre diğer ülkelere kıyasla toplamda ABD'nin çeşitli kurumları vasıtasıyla akademik çalışmalara oldukça aktif bir şekilde destek olduğu görülmektedir. Aktif destekte ABD'nin arkasından Çin ve Avrupa Komisyonu'nu gelmektedir.

**Tablo 6**
*En Fazla Yayın Gerçekleştiren Kurumlar.*

| Sıra | Kurum | Yayın Sayısı | Atıf Sayısı | Ülkesi |
|---|---|---|---|---|
| 1 | De Montfort Üniversitesi | 6 | 150 | İngiltere |
| 2 | King Saud Üniversitesi | 6 | 41 | Suudi Arabistan |
| 3 | King Abdulaziz Üniversitesi | 5 | 34 | Suudi Arabistan |
| 4 | Umm Al Qura Üniversitesi | 5 | 64 | Suudi Arabistan |
| 5 | California San Diego Üniversitesi | 5 | 53 | ABD |
| 6 | Vellore Teknoloji Enstitüsü | 5 | 161 | Hindistan |
| 7 | Edith Cowan Üniversitesi | 5 | 42 | Avustralya |
| 8 | Nevada Üniversitesi | 4 | 223 | ABD |
| 9 | Babasaheb Bhimrao Ambedkar Üniversitesi | 4 | 43 | Hindistan |
| 10 | Taif Üniversitesi | 4 | 37 | Suudi Arabistan |

VOSviewer ile oluşturulan Tablo 6'da alanda en fazla yayın gerçekleştiren kurumlara dair bilgiler verilmektedir. Yayın sayısı açısından ilk sırada De Montfort Üniversitesi yer almaktadır. Suudi Arabistan kurumlarının etkinliği dikkat çekmektedir ancak bu etkinliğe Suudi Arabistan kaynaklı yayınların bu listedeki belirli kurumlarda yoğunlaşmış olduğu değerlendirilebilir. En fazla yayın yapan ülke sıralaması göz önüne alınarak bu tabloya bakıldığında Suudi Arabistan'ın yayınlarının %48'i bu kurumlarca yapılmıştır. Bunula birlikte ABD ve Hindistan'ın ise yayınlarının ise farklı kurumlara dağıldığı değerlendirilebilir. Tablo 6 atıf sayıları açısından yorumlandığında ise oldukça değişkenlik göstermektedir. Tablo 6'daki ilk on ülkenin yalnızca ikisi atıf sayısında ilk on listeye girebilmektedir. Buna göre Hong Kong Üniversitesi 360 atıf ile ilk sırada yer almaktadır ve akabinde sırasıyla Salerno Üniversitesi (360 atıf), San Antonio Teksas Üniversitesi (360 atıf), Worcester Politeknik Enstitüsü (317 atıf), Illinois Teknoloji Enstitüsü (317 atıf), Singapur Ulusal Üniversitesi (254 atıf), Nevada Üniversitesi (223 atıf), Jyväskylä Üniversitesi (190 atıf), Oulu Üniversitesi (190 atıf) ve Vellore Teknoloji Enstitüsü (161 atıf) yer almaktadır. Atıf sayısında dört kurum ile çoğunluk yine ABD'ye aittir. Birer kurum ile diğer ülkeler ÇHC, İtalya, Hindistan ve Singapur'dur. Bu noktada dikkat çeken ülke Finlandiya olmaktadır. Jyväskylä Üniversitesi ve Oulu Üniversitesi ile Finlandiya listeye iki kurumunu sokmuştur.

**Tablo 7**
*En Fazla Yayın Yapan Yazarlar.*

| Sıra | Yazar | Yayın Sayısı | Atıf Sayısı |
|---|---|---|---|
| 1 | Helge Janicke | 4 | 71 |
| 2 | Arash Ghazvini | 4 | 20 |
| 3 | Zarina Shukur | 4 | 20 |
| 4 | Raees Ahmad Khan | 4 | 43 |
| 5 | Ying He | 3 | 41 |
| 6 | Alka Agrawal | 3 | 32 |
| 7 | Daniele Giansanti | 3 | 8 |
| 8 | Rajeev Kumar | 3 | 40 |
| 9 | Christian Dameff | 3 | 16 |
| 10 | Neil F. Doherty | 2 | 74 |

Tablo 7'de en fazla yayın sayısına sahip ilk on yazar ifade edilmektedir. İlk sırada yer alan Helge Janicke atıf sayısı açısından aynı performansı gösterememiştir. Atıf sayısında diğer yazarlara göre geri kalmıştır. Bu noktada en fazla atıf sayısına sahip yazar İtalya, Salerno Üniversitesi'nden Christian Esposito olmaktadır. Bir yayını bulunan yazarın Alfredo De Santis, Genny Tortora, Henry Chang ve Kim-Kwang Raymond Choo ile birlikte yayımladığı "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" çalışma toplam 359 atıf almıştır. Bu bakımdan Christian Esposito'nun bu çalışmada birinci yazar olması dolayısıyla alanda en fazla atıfa sahip yazar olduğu kabul edilmiştir. Dörder yayına sahip ilk dört yazarın sağlık kurumlarında bilgi güvenliği yönetiminde hangi konuları çalıştığının değerlendirilmesi amacıyla çalışmalarının özetleri incelenmiştir. İncelemede Helge Janicke'nin alanı daha geniş bir perspektifte bütüncül olarak incelediği, Zarina Shukur ve Arash Ghazvini'nin dört yayını da ortak yazdığı ve Raees Ahmad Khan'ın ise konuya mühendislik bakış açısından yaklaştığı görülmüştür.

Helge Janicke bir makalesinde sağlıkta nesnelerin interneti kapsamında siber güvenlik sağlanması için "federe derin öğrenme yaklaşımları"nı ele alan deneysel bir araştırma çalışmıştır. Bu çalışmasında nesnelerin interneti araçlarının olası siber saldırıları tespit ederek veri gizliliğini sağlama düzeyini arttırmayı amaçlamıştır. Yazar diğer üç makalesinde ise konunun teknik yönünden uzaklaşarak sosyal bilimler ile ilişkili yönlerine eğilmiştir. Bu makalelerin ikisinde sağlıkta bilgi güvenliği ihlaline yol açan en büyük faktörün insan hatası olduğu varsayımından yola çıkarak ihlale yol açan insan hatalarının tespit edilmesi için vaka çalışması yürütmüştür. Yazar bu iki çalışmasının birinde retrospektif kayıt incelemesi yaparken birinde kesitsel çalışma yapmıştır. Ancak iki çalışmasında da "İnsan Hatası Değerlendirme ve Azaltma Tekniği"nin (Human Error Assessment and Reduction Technique - HEART) bilgi güvenliğine uyarlanmış hali olan "Bilgi Güvenliği Temel İnsan Hatası Nedenleri" (Information Security Core Human Error Causes - IS-CHEC) ölçme aracının sağlık kurumlarında bilgi güvenliği yönetimi çalışmalarının iyileştirilmesinde kullanışlı bir araç olabileceği değerlendirmesini yapmaktadır. Janicke, dördüncü makalesinde ise bilgi güvenliğinin etik kavramı ile olan ilişkisini ele alarak konuya teorik bir bakış açısı getirmiştir. Buna göre bilgi güvenliğinin "ahlaki değere" sahip olabileceğini ifade ederek eleştirel teorinin olası etik sorunların daha iyi anlaşılmasını kolaylaştırabileceği ve bu sorunları ele alma yollarını bulurken destek sağlayabileceği öne sürmüştür. Yazar bu teorisini Birleşik Krallık'ın elektronik sağlık kayıtları sisteminde örneklendirmiştir.

Her dört yayında beraber çalışan diğer yazarlar Arash Ghazvini ve Zarina Shukur ise bilgi güvenliği konusunun "personel eğitimi" noktasında çalışmalar gerçekleştirmişlerdir. Sağlık kurumlarında bilgi güvenliği yönetimini elektronik sağlık kayıtlarına indirgeyen yazarlar Helge Janicke'ye benzer şekilde en büyük ihlal sebebinin insan hataları olduğu varsayımından yola çıkarak insan hatalarını azaltma amacıyla sağlık profesyonelleri için bilgi güvenliği eğitim modelleri geliştirilmesine odaklanmışlardır. Bu doğrultuda Ghazvini ve Shukur'ün çalışma konuları bilgi güvenliği eğitimi için eğitim içeriği ve rehber kılavuz tasarlamak, eğitimler için ihtiyaç ve başarı

faktörlerini tespit etmek ve eğitimde oyunlaştırmada "ciddi oyun" (serious game) geliştirmek olmuştur. Alanda bilgi güvenliği mühendisliği bakış açısıyla çalışan Raees Ahmad Khan sağlık bilgi sistemlerinin güvenliğinin değerlendirilmesi ve iyileştirilmesi için mühendislik alanına dair geliştirilmiş farklı teknikleri kullanarak çok faktörlü çalışmalar yapmıştır. Çalışmalarının birisinde siber güvenlik açısından sağlık bilgi sistemlerinin çoğunlukla simetrik mekanizmalarının hedef alındığını belirtmiştir. AHP-TOPSIS yönteminin hibrit bulanık tabanlı simetrik metodolojisini kullanarak bilgi güvenliği ihlaline yol açan faktörleri tespit ederek karşılaştırma ve duyarlılık analizleri ile değerlendirilmesini amaçlamıştır. Yazar teorik olarak benzer çerçevede yaptığı diğer çalışmalarında ise Bulanık Analitik Hiyerarşi Prosesi (Fuzzy AHP), Çok Kriterli Karar Verme tabanlı Analitik Hiyerarşi Süreci, TOPSIS ve Makine Öğrenmesi yöntemlerini kullanmıştır. Teorik olarak benzer çerçevede ilerleyen yazar sağlık büyük veri ve hastane bilgi sistemleri ile çalışmıştır. Yazarın son çalışma konusu ise Covid-19 pandemisi olmuştur. Küresel etkisi olan Covid-19 pandemisinin dijitalleşme açısından yol açtığı değişimler doğrultusunda siber güvenlik konusundaki gelişmeleri incelemiştir.

**Tablo 8**
*En Fazla Atıf Alan Yayınlar.*

| Sıra | İlk Yazar | Yayın Yeri | Yayın Yılı | Yayın Başlığı | Atıf Sayısı |
|---|---|---|---|---|---|
| 1 | Esposito, C. | IEEE Cloud Computing | 2018 | Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? | 360 |
| 2 | Li, M. | IEEE Wireless Communications | 2010 | Data Security and Privacy in Wireless Body Area Networks | 317 |
| 3 | Moody, G. D. | MIS Quarterly | 2018 | Toward A Unified Model of Information Security Policy Compliance | 176 |
| 4 | Dehling, T. | JMIR mHealth and uHealth | 2015 | Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android | 133 |
| 5 | Pfleeger, SL | Computers & Security | 2012 | Leveraging Behavioral Science to Mitigate Cyber Security Risk | 111 |
| 6 | Tsohou, A. | Computers & Security | 2015 | Analyzing The Role of Cognitive and Cultural Biases in The Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs | 110 |
| 7 | Wilkowska, W. | Health Informatics Journal | 2012 | Privacy And Data Security in e-Health: Requirements from The User's Perspective | 110 |
| 8 | Anand, A. | Computer Communications | 2020 | An Improved DWT-SVD Domain Watermarking for Medical Information Security | 106 |
| 9 | Luxton, DD. | Telemedicine and e-Health | 2012 | mHealth Data Security: The Need for HIPAA-Compliant Standardization | 86 |
| 10 | Hedstrom, K. | Journal of Strategic Information Systems | 2011 | Value Conflicts for Information Security Management | 81 |

Alanda en fazla atıf alan yayınlara ise Tablo 8'de yer verilmektedir. En fazla atıf alan yayınlar aynı zamanda en fazla atıf alan yazarlara işaret ederek bu yazarlar için bilgi içermektedir. İlk bakışta IEEE ve Elsevier'in rekabeti yazar bazında da göze çarpmaktadır. Ayrıca ilk on çalışmanın toplam atıf sayısı 1 590'dır. Bu rakam oransal olarak alandaki toplam atıf sayısının (n=5 194) %30.61'ine tekabül etmektedir. Bu açıdan %30'luk bir oranın nispeten düşük olmadığını göz önüne alarak bir değerlendirme yaptığımızda alandaki atıf sayılarının yığılma yerine dağılım gösterdiği düşünülebilir. En fazla atıf alanlar olması dolayısıyla bu yayınların alandaki bilimsel üretim için doğal referans kaynakları olduğu kabul edilirse hangi konuları kapsadıkları ve alana katkılarının değerlendirilmesi önemli olmaktadır. Ancak bu değerlendirmeye ilk beş yayın detaylı olarak dahil edilmiştir. İlk beş yayının atıf oranı bu ilk on yayının %69'una tekabül etmektedir. Bu açıdan ilk beş yayının ağırlığı oldukça yüksektir.

Esposito ve ark. (2018) ilk sırada yer alan "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" çalışmalarında bulut bilişimin sağlık hizmetlerindeki kullanım durumunu bulut bilişimin halihazırda sunabildiği bilgi güvenliği koruma yöntemleri ile karşılıklı olarak değerlendirmişlerdir. Esposito ve ark.'na göre bulut bilişim, bilişim teknolojilerindeki ilerlemeye göre veri güvenliğini sağlamada dezavantajlı pozisyondadır. Yazarlar bu durumdan dolayı çalışmalarında bulut bilişim teknolojisinin artık blockchain teknolojisi ile ikame edilebileceğini teorik olarak çeşitli yönlerden tartışmaktadırlar.

Li ve ark. (2010) "Data Security and Privacy in Wireless Body Area Networks" başlıklı çalışmalarında "Kablosuz Vücut Alan Ağları"nı (WBAN) bilgi güvenliği açısından tartışmışlardır. Yazarlar WBAN sistemlerinin bilgi güvenliğinin sağlanmasında zorluklar olduğunu ileri sürmüşlerdir. Li ve ark. WBAN sistemleri için geliştirilen güvenlik çözümlerini incelemiş ve kullanılabilirliklerini analiz etmişlerdir. Bu noktada uygulama örnekleri veren yazarlar bilgi güvenliğini iki farklı bağlamda ele almışlardır: "güvenli ve güvenilir dağıtık veri depolama" ve "hassas ve özel hasta sağlık verileri için ince taneli dağıtık veri erişim kontrolü".

Moody ve ark. (2018) "Toward A Unified Model of Information Security Policy Compliance" çalışması bilgi güvenliğinin davranış bilimleri ile ilişkisini inceleyen bir araştırmadır. Yazarlar bilgi güvenliği davranışına etki eden on bir farklı sağlık davranış modelini (sağlık inanç modeli, koruma motivasyonu teorisi, kontrol dengesi teorisi vb.) ampirik olarak incelemiş ve bu teorileri bütünleştiren yeni bir teori modeli öne sürmüşlerdir ve test etmişlerdir. Yazarların öne sürdüğü model "Birleşik Bilgi Güvenliği Politikası Uyum Modeli (Unified Model of Information Security Policy Compliance - UMISPC)"dir. Moody ve ark. (2018) geliştirdikleri modelin bilgi güvenliğini davranışlarını açıklamak için kullanılabileceğini ifade etmektedirler.

Dehling ve ark. (2015) "Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android" çalışmalarında mobil sağlık uygulamalarında bilgi güvenliği konusunu çalışmışlardır. Android ve iOS'ta yer alan "tıp" ile "sağlık ve fitness" kategorilerindeki uygulamalara dair olası bilgi güvenliği ihlallerinin kullanıcılar için doğurabileceği potansiyel zararlara odaklanıldığı belirtilmektedir. Bu bakımdan uygulamalar çeşitli kategorilerde incelenmiş ve potansiyel zarar düzeyine göre kategorize edilmiştir.

Pfleeger ve Caputo (2012)'nun "Leveraging Behavioral Science to Mitigate Cyber Security Risk" çalışmasında bilgi güvenliğinde davranış bilimi bakış açısıyla insan hatasını ele almışlardır. Yazarlar insan davranışını anlamanın siber güvenlikte etkinliği yükselttiğini ifade etmektedirler. Buna göre davranış bilimlerinin uygulanması siber güvenliğin sağlanmasında çok önemli olmaktadır.

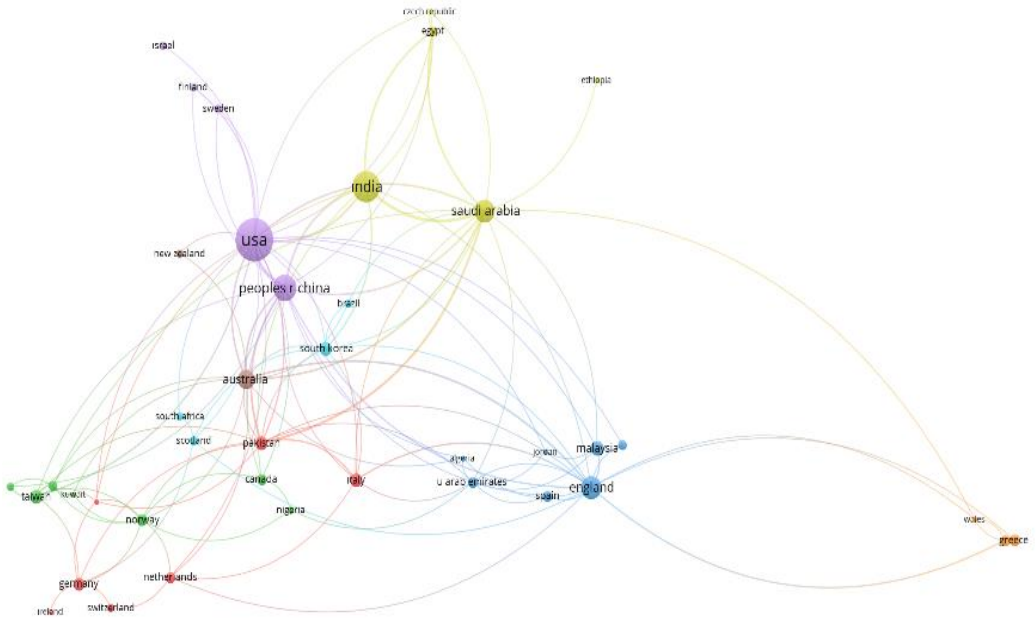
Diğer yazarlar ise Tsohou ve ark. (2015) bilgi güvenliği algı ve davranışlarını incelemek; Wilkowska ve Ziefle (2012) güvenlik ve mahremiyet odağında bireylerin teknoloji kullanımı gereksinimlerini belirlemek; Anand ve Singh (2020) DWT-SVD Tabanlı Resim Damgalama yöntemi ile hasta görüntülerine çoklu-filigranlar gömerek bilgi güvenliğini sağlayan filigranlama tekniği çalışmak; Luxton ve ark. (2012) ABD'de "Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (Health Insurance Portability and Accountability Act - HIPAA) çerçevesinde mevcut güvenlik ihtiyaçlarına ve zorluklara dair bakış açısı sağlamak; Hedstrom ve ark. (2011) sağlık kurumları bilgi güvenliği yönetimi için değer temelli uyum modeli önerisi geliştirmek başlıklarını çalışmışlardır.

**Bibliyometrik Analizler**

Ülkeler eş yazarlık bağlamında analiz edildiğinde oluşan ilişki ağı Şekil 3'te gösterilmektedir. Analizde her bir ülkenin en az iki yayını ve beş atıfı olmasına dikkat edilmiştir. Buna göre 64 ülkeden 43'ü bu kriterleri karşılamaktadır. VOSviewer ile yapılan analizde toplam on bir ilişki bulutu oluşmaktadır. On bir bulut içerisinde yedi ülkeden oluşan üç farklı bulut bulunmaktadır. Bunlar aynı zamanda analizdeki en büyük ilişki bulutlarıdır. Birinci bulut Kanada, Kuveyt, Nijerya, Norveç, Singapur, Tayvan ve Türkiye'den oluşmaktadır. İkinci bulut Cezayir, İngiltere, İran, Ürdün, Malezya, İspanya ve Birleşik Arap Emirlikleri'dir. Üçüncü bulut ise Almanya, İrlanda, İtalya, Hollanda, Pakistan, İsviçre ve Vietnam'dır. Ayrıca Ekvador, Danimarka ve Ukrayna'dan oluşan üç ülke eş yazarlığa gitmemiştir. Bu bağlamda bu üç ülke çıkarıldığında birbiri ile etkileşimli 40 ülkeden oluşan analiz sonucu aşağıdaki Şekil 3'te gösterilmiştir.

**Şekil 3**

Ülkelere Göre Eş Yazarlık Analizi




Analiz sonucunda ABD 22 farklı ülke ile eş yazarlığa giderek en fazla eş yazarlık gerçekleştiren ülke olmaktadır. Bu açıdan ABD en fazla iş birliği gerçekleştiren ülkedir. ABD'nin ardından eş-yazarlık sıralamasında sırasıyla İngiltere (16), ÇHC (15), Suudi Arabistan (15) ve Avustralya (13) ülkeleri gelmektedir. Eş yazarlık analizi VOSviewer ile kurum perspektifinde de yapılmıştır. Analizde her bir kurumun en az iki yayını ve beş atıfı olmasına dikkat edilmiştir. Buna göre 662 kurumdan 76'sı bu kriterleri karşılamaktadır ve toplam 39 ilişki bulutu oluşmaktadır. Ancak 76 kurumdan 26'sı eş yazarlık

gerçekleştirmemiştir. Şekil 4'te ise 14 kurumdan oluşan en büyük ilişki ağı gösterilmektedir. Şekil 4'e göre California San Diego Üniversitesi ve Harvard-MIT Center for Regulatory Science beşer iş birliği ile en fazla eş yazarlık gerçekleştiren kurumlar olmaktadır.

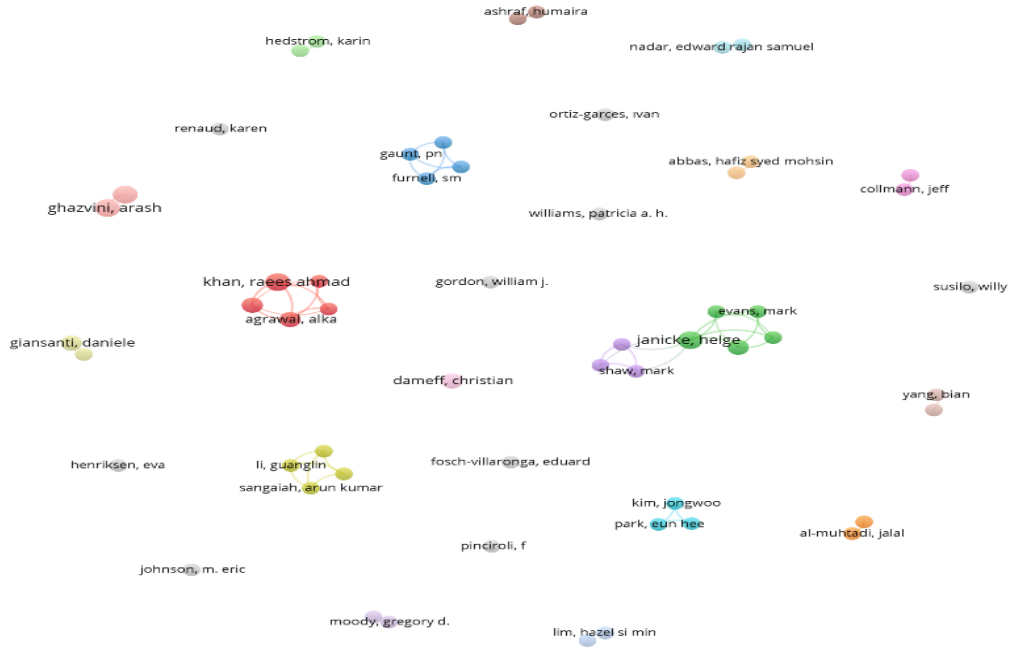
**Şekil 4**

Kurumlara Göre Eş Yazarlık Analizi


Yazarların eş yazarlık incelemesi her bir yazarın en az iki yayını ve beş atıfı olması kriterleri doğrultusunda VOSviewer programı ile yapılmıştır. Buna göre alandaki 1 197 yazardan 56'sı bu kriterleri karşılamaktadır ve toplam 27 farklı eş yazarlık bulutu oluşmuştur. Ancak toplam 10 farklı yazar eş yazarlık gerçekleştirmemiştir. VOSviewer'e göre en büyük ilişki ağı 8 yazardan oluşmaktadır. Bu durumun toplam yazar sayısı olan 56'ya göre düşük olması açısından analiz sonucunu tam yansıtabilmek adına Şekil 5'te 27 bulutun tamamına yer verilmiştir.

**Şekil 5**

Yazarlara Göre Eş Yazarlık Analizi




Şekil 5'te beşer yazardan oluşan iki en büyük bulut bulunmaktadır. Raees Ahmad Khan, Rajeev Kumar, Abdullah Baz, Hosam Alhakami ve Alka Agrawal bir bulutu oluştururken diğer bulut Mark Evans, Ying He, Helge Janicke, Leandros Maglaras ve Iryna Yevseyeva'dan oluşmaktadır. Helge Janicke ve Raees Ahmad Khan'ın dörder yayınla aynı zamanda en fazla yayın yapan yazarlar olması hasebiyle bilgi güvenliği yönetimi alanında çalışan yazarların üretkenlikleri için iş birliklerinin pozitif etki yaptığı değerlendirilebilir. Nitekim en fazla atıf alan on yayının tamamı birden fazla yazar

içermektedir. VOSviewer ile anahtar kelimeler üzerinden eş birliktelik analizi yapılmıştır. Eş birliktelik analizinin tüm aşamalarında her bir anahtar kelimenin en az beş kere görülmesi dahil edilme kriteri olarak belirlenmiştir. Bu doğrultuda yapılan analiz sonucunda 1 157 anahtar kelimeden 34'ü dahil edilme kriterini karşılamaktadır. En sık görülen ilk on anahtar kelimeye Tablo 9'da yer verilmektedir. Görüldüğü üzere "cybersecurity" anahtar kelimesi açık ara en fazla kullanılan anahtar kelime olmaktadır.

**Tablo 9**

*Anahtar Kelimeler Eş Birliktelik Analizi.*

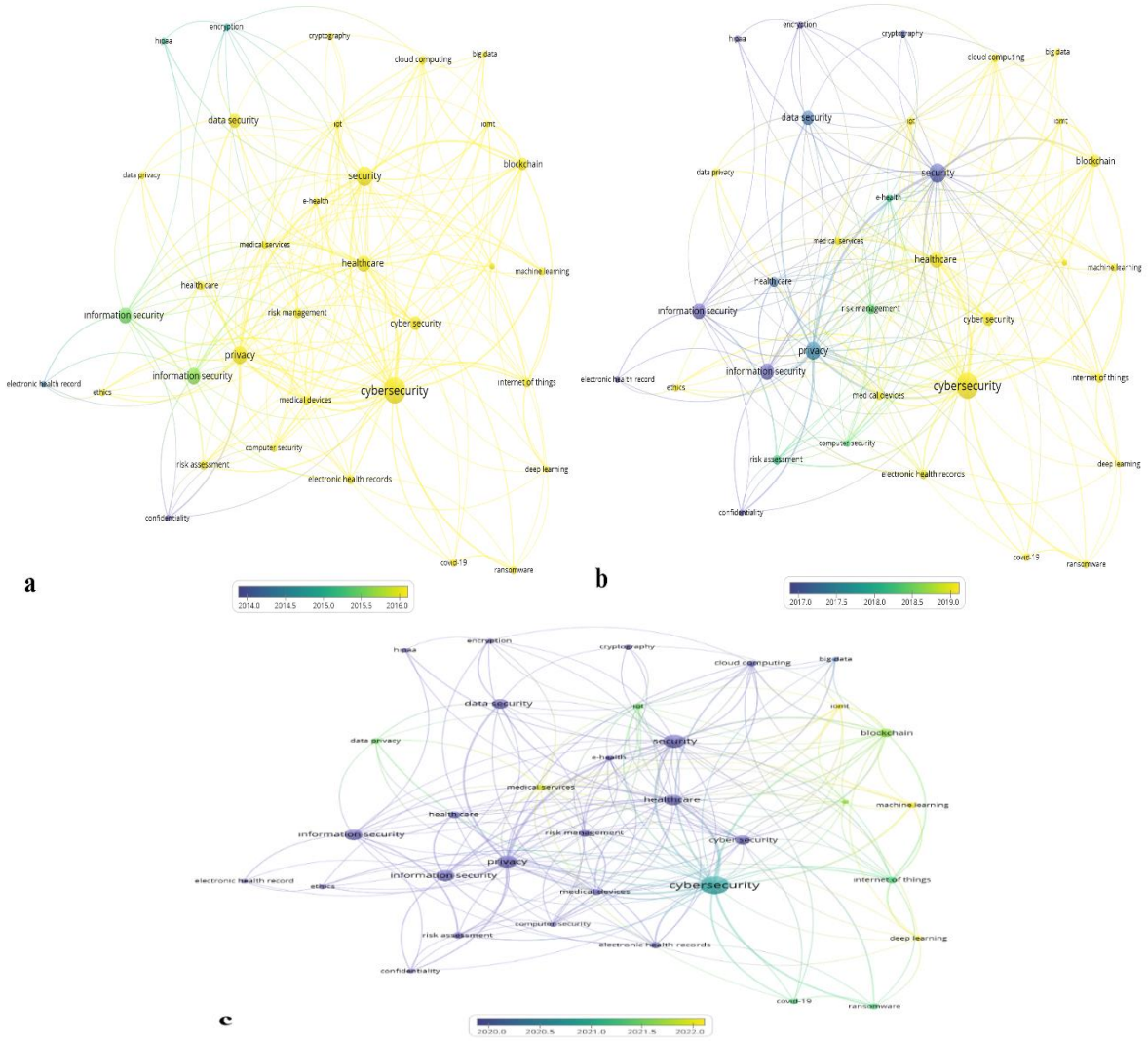
| | Sıra | Anahtar Sözcük | Görülme Sıklığı | | Sıra | Anahtar Sözcük | Görülme Sıklığı |
|---|---|---|---|---|---|---|---|
| **Benzerlik İncelemesi Öncesi** | 1 | cybersecurity | 72 | **Benzerlik İncelemesi Sonrası** | 1 | cybersecurity<br>cyber security | 92 |
| | 2 | security | 42 | | 2 | information security<br>ınformation security | 56 |
| | 3 | privacy | 35 | | 3 | ınternet of things<br>ıomt | 44 |
| | 4 | information security | 29 | | 4 | ıot<br>security | 42 |
| | 5 | healthcare | 28 | | 5 | healthcare<br>health care | 39 |
| | 6 | ınformation security | 27 | | 6 | privacy | 35 |
| | 7 | data security | 23 | | 7 | data security | 23 |
| | 8 | cyber security | 20 | | 8 | blockchain | 16 |
| | 9 | blockchain | 16 | | 9 | electronic health record<br>electronic health records | 15 |
| | 10 | risk management | 11 | | 10 | risk management | 11 |

Tablo 9'un iki farkı boyutu bulunmaktadır. Anahtar kelimelerin kullanımına yönelik yapılan incelemede kelimelerin benzer farklı kullanımlarının yazarlar tarafından tercih edildiği görülmüştür. Bu durum dolayısıyla anahtar kelimeler üzerinde ayrıca benzerlik incelemesi de yapılmıştır. İnceleme sonucunda benzer farklı kullanımlar bir araya getirilerek sıklıkları belirlenmiştir. Ancak benzer farklı kullanımların olmasına rağmen ilk on anahtar kelimenin dağılımında ilk listeden eksilme olmadığı ve hatta ikinci liste için iki yeni anahtar kelimenin eklendiği görülmektedir.

Benzerlik incelemesinde öncelikle ilk on içerisindeki kelimelere bakıldığında "cybersecurity" ve "cyber security" şeklinde iki farklı kullanım göze çarpmaktadır. İlk on içerisinde bir başka benzer kullanım örneği bilgi güvenliği kavramında görülmektedir. Bilgi güvenliği "information security" ve "ınformation security" olmak üzere iki farklı şekilde kullanılmaktadır. İlk on içerisindeki bir başka kelime olan "healthcare" anahtar kelimesinin de farklı bir kullanımı bulunmaktadır. Bu kullanım "health care" (11 kez) şeklindedir. Kullanımı en değişken olan anahtar kelimenin nesnelerin interneti kavramı olduğu kabul edilebilir. Nitekim ilk listede sıralamaya giremese de benzerlik incelemesi sonrası üçüncü sıraya girmiştir. Nesnelerin interneti için kullanılan farklı kelimeler "ınternet of things" (10 kez), "ıot" (19 kez) ve "ıomt" (15 kez) şeklindedir. Bir başka farklı kullanım şekli ise "electronic health record" (5 kez) ve "electronic health records" (10 kez) kavramlarında görülmektedir.

**Şekil 6**

*Dönem Aralıklarına Göre Anahtar Kelimeler Dağılımı. (a) 2014-2016 Dönemi. (b) 2017-2019 Dönemi. (c) 2020-2022 Dönemi.*




Anahtar kelimelerin dağılımında toplam beş bulut oluşmaktadır. En büyük bulut on kelimeden oluşmaktadır. Bunlar computer security, confidentiality, electronic health record, ethics, information security, ınformation security, medical devices, privacy, risk assessment, risk management anahtar kelimeleridir. Sekiz anahtar kelimelik ikinci bulutta ise artificial intelligence, blockchain, cryptography, cyber security, e-health, ıomt, ıot ve security'dir.

Eş birliktelik analizinde son olarak zaman dönemlerine göre bir inceleme yapılmıştır. Bu inceleme ile anahtar kelimelerin zamansal değişimleri belirlenmeye çalışılmıştır. Anahtar kelimelerin zamansal değişimi ile alanda çalışılmakta olan en güncel konu başlıklarının tespit edilmesi amaçlanmıştır. Buna göre 2014-2016, 2017-2019 ve 2020-2022 olmak üzere üç farklı dönem aralığında inceleme yapılmıştır.

Şekil 6'yı oluşturan üç alt grafiğe birlikte bakıldığında alanda zamana dayalı olarak değişimlerin yaşandığı görülmektedir. İlk olarak 2014-2016 dönemine bakıldığında confidentiality, electronic health record ve encryption kavramlarının eskimeye başladığı görülmektedir. Sık kullanılan anahtar kelimeler bu dönem için güncel çalışılan kavramlar olduğu görülmektedir. Bu bakımdan 2014-2016 döneminde çalışılan alanlar elektronik sağlık kayıtları-gizlilik-kriptografi olmaktadır.

2017-2019 döneminde ise alanda değişim açık olarak görülmektedir. Bir önceki döneme göre alanda yeni kabul edilen kavramların çoğu eskimeye başlamıştır. Bunlar arasında privacy, security, data security, risk assesment, computer security, risk management ve information security yer almaktadır. Buna göre 2017-2019 döneminde çalışılan alanlar veri gizliliği/güvenliği-risk değerlendirme/yönetimi-bilgi güvenliği olmaktadır.

Son dönem 2020-2022 aralığında ise alanda güncelliği koruyan anahtar kelime sayısının sınırlı olduğu görülmektedir. Alanda en güncel anahtar kelimeler deep learning, machine learning, ınternet of medical things ve medical services'dir. Sağlık bilişimi açısından güncel kavramlar olarak düşünülen artificial intelligence, blockchain, internet of things ve ransomware'nin dahi bu kavramlara göre güncelliği azalmaktadır. Bu bakımdan alanda son dönem itibariyle güncel çalışma alanları derin öğrenme-makine öğrenmesi-medikal nesnelerin interneti olmaktadır.

Anahtar kelimeler üzerinden yapılan bu incelemede alandaki değişimin oldukça hızlı yaşandığı görülmüştür. Şekil 6'da da görsel olarak bu durum görülmektedir. Yayın ve atıf sayılarının yıl bazındaki dağılımını veren Grafik 1'e bakıldığında yayın sayılarında son dönemlerde ani artış görülmektedir. Bu açıdan alandaki hızlı değişimin nedeni bu durum ile açıklanabilir. Alandaki çalışma hızı oldukça yüksek olmaktadır ve bu durum kavramların hızlı bir şekilde eskimesine neden olmaktadır. Bu durum aynı zamanda teknolojik gelişmelerin hızlı olmasının da doğal bir sonucu olarak kabul edilebilir.

## TARTIŞMA

Bibliyometrik araştırma yönteminin kullanıldığı çalışmada sağlık kurumlarında bilgi güvenliği konusunda yapılan akademik çalışmalar farklı analiz türlerinde incelenmiş ve literatürün mevcut durumu ortaya konulmuştur.

Alanın en etkin dergilerinin yayın kategorilerindeki dağılımı açısından sağlıkta bilgi güvenliği yönetimi alanında yayın yapan dergiler sağlık bilişimi ağırlıklı dergilerdir. Dergilerin yayımlamış oldukları yayınlar ve öne çıkan yayınların kategorilerine bakıldığında bilişim ve mühendislik odaklı olduğu görülmüştür. Bu durum araştırma konusunun bilgi güvenliği olması açısından doğal bir sonuç olarak yorumlanabilir. Araştırma sonuçlarına göre yayın ve atıf sayılarının da bu durumdan etkilendiği söylenebilir. Mühendislik açısından teknolojide yaşanan gelişmelere ve toplumdaki kullanım yaygınlığına dayalı olarak yayın ve atıf sayılarında yıllar itibariyle değişimler olmuştur. Literatürde bilgi ve iletişim teknolojilerinin 2010'lu yıllardan sonra büyük bir gelişme gösterdiği (T.C. Kalkınma Bakanlığı, 2018) ve yine aynı dönemlerde toplumda da giderek artan bir şekilde yaygınlığın gözlemlendiği belirtilmektedir (Arslankara ve Usta, 2020). Bu bağlamda yayın ve atıf sayılarındaki yoğunlaşmanın belirtilen dönem sayıları ile paralel olduğu görülmektedir. Atıf sayısında 2020-2021'deki yaşanan sıçrama ve pik noktasında ise Covid pandemisinin etkili olduğu düşünülebilir. Pandemi sürecinde yaşanan kapanma dönemi ve sağlık hizmetinde sunumundaki değişen koşullar hizmetin neredeyse tamamen bilişim sistemleri ile sunulmasına yol açmıştır (İleri ve Kara, 2022). Bu açıdan teknolojideki bu ilerleme eğilimi doğrultusunda yayın ve atıf sayıları açısından alanda ilerlemenin süreceği düşünülmektedir. Ancak bu noktada alanın tamamen mühendislik bakış açısıyla şekillendiğini söylemek doğru olmayacaktır. Öne çıkan yayınların azımsanmayacak bir kısmı konunun

sosyal yönlerine odaklanmaktadır. Aynı zamanda dergilerin bu çerçevede de yayınlara yer verdiği görülmüştür. Sosyal açıdan alanda en çok davranış bilimleri ile ilişki kurulduğu görülmüştür. Alanda yaygın bir varsayım olarak insan hataları bilgi güvenliği ihlallerinde en yaygın nedenler arasında görülmüş bu hataların tespit edilip asgariye indirilmesi için çeşitli çalışmalar yapılmıştır.

Alandaki dergi dağılımında IEEE tarafından yayınlanan dergiler ön planda yer almaktadır. Hem yayın sayısı hem de atıf sayısı açısından IEEE güçlü bir konumda bulunmaktadır. IEEE'nin yayınlandığı dergiler ile alanda oldukça etkin olduğu değerlendirilmektedir. Bu açıdan alanda yeni çalışmalar yapacak araştırmacıların dergi tercihinde IEEE'nin ilk sırada yer alacağı düşünülmektedir. Siber fiziksel sistemler ve siber güvenlik üzerine yapılan bir çalışmada da IEEE'nin alanda önde gelen bir yayıncı olduğu değerlendirilmektedir (Yıldız ve Gejam, 2022). Ülkeler noktasında bir değerlendirme yapıldığında ABD alanda öncü ülke konumundadır. ABD ayrıca akademik çalışmalara en fazla finansal kaynak sağlayan ülkedir. Bu açıdan ABD'nin en fazla yayın ve atıf sayısına sahip olması bu durum ile birlikte değerlendirilebilir. Bir başka ifade ile alanda etkili olmanın bilimsel araştırmalara sağlanan destek miktarı ile ilişki olduğu değerlendirilebilir. Nitekim konuyla ilgili en fazla yayın yapan ülkelerin çoğunluğunun kendi ülkelerinden finansal destek aldığı görülmektedir. Bu bakımdan alanda yapılacak akademik çalışmalara verilen finansal destek miktarının araştırma verimliliği ile doğrudan ilişkili olduğu değerlendirilmektedir. Bu değerlendirmede ayrıca iş birliklerinin bu ilişkide etkili olduğu düşünülebilir. Şekil 3 bağlamında bakıldığında ABD en fazla eş yazarlık gerçekleştiren ülke olarak iş birliklerinde de ilk sırada yer almaktadır. Nitekim iş birliğinde önde gelen diğer ülkelerin de aynı zamanda yayın ve atıf sayısında ön planda yer alan ülkeler olduğu görülmektedir.

Çalışmada önemli bir tartışma olarak düşünülen bir diğer noktanın ise anahtar kelimelerin kullanımındaki mevcut durum olduğu düşünülmektedir. Tablo 9'da yer verildiği üzere alandaki araştırmacıların anahtar kelime kullanımlarında şekil farklılıkları gözlenmektedir. Bu farklılar "health care"-"healthcare", "information security"-"ınformation security" veya "ıot"-"ıomt" gibi birbirine oldukça benzer farklılıklar olmaktadır. Bu bakımdan araştırmacıların anahtar kelime kullanımı tercihlerinde terimsel olarak birbirine benzer nitelikte farklılaşmanın var olduğu görülmektedir. Bu açıdan terimsel ortaklık sağlanması adına standartlaştırma çalışmalarının kullanımının önemini ortaya koymaktadır.

## SONUÇ VE ÖNERİLER

Bu çalışmada literatür betimlenmesi amacı doğrultusunda "sağlık kurumlarında bilgi güvenliği" konusunda yapılan akademik çalışmalar incelenmiş ve değerlendirmelerde bulunulmuştur. Alan teknolojik gelişmelere paralel olarak ilerlemektedir. Bununla birlikte durumsal koşulların da etkisi ile son dönemde oldukça güncel çalışılan bir alan olmaktadır. Sonuç olarak sağlıkta bilgi güvenliğinin teknik boyutunun yanı sıra hukuki, etik ve örgütsel (personel algısı, dijital okuryazarlık vb.) boyutlarını ele alan daha fazla ve geniş kapsamlı çalışmalar yapılmasının alana katkı sağlayacağı değerlendirilmektedir.

## SINIRLILIKLAR

Yöntem kısmında görüldüğü üzere bir bibliyometrik olan araştırmanın sınırlıkları olarak yalnızca WoS veri tabanı kullanılması, spesifik anahtar kelimeler kullanılması, WoS veri tabanında yalnızca makale ve erken erişim kategorileri kullanılması, yalnızca İngilizce yayın dili kullanılması ve dönem aralığı sınırlaması kullanılması (1982-28.5.2023) ifade edilebilir.

**Etik Onay**

Çalışmanın, hazırlık, bilgi sunumu, literatür tarama, yazım olmak üzere tüm aşamalarında bilimsel ve etik kurallara uygun davranılmıştır. Çalışma kapsamında kullanılan tüm veri ve bilgilerde kaynak gösterimine dikkat edilmiş ve çalışma Commite on Publication Ethics (COPE)'in tüm şartlarına uygun ve Dünya Tıp Birliği (WMA) Helsinki Bildirgesi gözetilerek yapılmıştır.

**Çıkar Çatışması**

Çıkar çatışması yoktur.

**Finansal Destek**

Finansal destek yoktur.

**Yazar Katkıları**

Tasarım: Y.Y.İ., M.Y.A., Veri toplama veya veri girişi yapma: Y.Y.İ., M.Y.A., Analiz ve yorum: Y.Y.İ., M.Y.A., Literatür tarama: Y.Y.İ., M.Y.A., Yazma: Y.Y.İ., M.Y.A.

## KAYNAKLAR


Abouelmehdi, K., Beni-Hessane, A. & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data, 5*(1). https://doi.org/10.1186/s40537-017-0110-7

Altındiş, S. (2012). Sağlık hizmetlerinde bilgi yönetimi. *SD Platform, Sağlık Düşüncesi ve Tıp Kültürü Dergisi, 23*, 90-91. https://medipol.com.tr/medium/Publication-File-123.vsf

Anand, A. & Singh, A. K. (2020). An improved dwt-svd domain watermarking for medical information security. *Computer Communications, 152,* 72-80. https://doi.org/10.1016/j.comcom.2020.01.038

Arslankara, V. B. & Usta, E. (2020). Lise Öğrencilerinde Sanal Risk Algısı: Problemli İnternet Kullanımı ve Eleştirel Düşünme Bağlamında Bir Araştırma. *Necmettin Erbakan Üniversitesi Ahmet Keleşoğlu Eğitim Fakültesi Dergisi (AKEF), 2*(1), 134-153. https://dergipark.org.tr/tr/download/article-file/1173051

Bahar, A., Özgürbüz, N., Erdem, D. T. & Dulkara, G. H. (2022). Hemşirelik ve Ebelik Öğrencilerinin Hasta Mahremiyeti Bilincine İlişkin Bilgi ve Tutumlarının İncelenmesi. *Necmettin Erbakan Üniversitesi Genel Sağlık Bilimleri Dergisi, 4*(2), 118-129. https://dergipark.org.tr/tr/download/article-file/2298374

Baran, S. & Şener, E. (2019). Hastanelerde bilgi güvenliği yönetimi: nitel bir araştırma. *Süleyman Demirel Üniversitesi Vizyoner Dergisi, 10*(23), 108-125. https://doi.org/10.21076/vizyoner.444451

Bundesamt für Sicherheit in der Informationstechnik. (2020, September 17). Newsletter SICHER • INFORMIERT vom 09.09.2021. https://www.bsi.bund.de/SharedDocs/Newsletter/DE/BuergerCERT-Newsletter/16_Sicher-Informiert_09-09-2021.html

Cahit Arf Bilgi Merkezi. (t.y.). Bibliyometrik Analiz Sıkça Sorulan Sorular: Bibliyometri Nedir? https://cabim.ulakbim.gov.tr/bibliyometrik-analiz/bibliyometrik-analiz-sikca-sorulan-sorular/

Chen, C. (2017). Science mapping: a systematic review of the literature. *Journal of Data and Information Science, 2*(2), 1–40. https://doi.org/10.1515/jdis-2017-0006

Dehling, T., Gao, F., Schneider, S. & Sunyaev, A. (2015). Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android. *JMIR mHealth and uHealth, 3*(1), e8. https://doi.org/10.2196/mhealth.3672

Deniz, M. Ö. (2023). Kişisel Verilerin İşlenmesi Sözleşmesinin Türleri ve Hukuki Nitelikleri. *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi (NEÜHFD), 6*(1), 97-114. https://dergipark.org.tr/tr/download/article-file/2637108

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N. & Lim, W. M. (2021). How to conduct a bibliometric analysis: an overview and guidelines. *Journal of Business Research, 133,* 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Esposito, C., De Santis, A., Tortora, G., Chang, H. & Choo, K. K. R. (2018). Blockchain: a panacea for healthcare cloud-based data security and privacy?. *IEEE Cloud Computing, 5*(1),31-37. http://dx.doi.org/10.1109/MCC.2018.011791712

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems, 20*(4), 373-384. https://doi.org/10.1016/j.jsis.2011.06.001

Hou, Q., Mao, G., Zhao, L. & Du H, Zuo J. (2015). Mapping the scientific research on life cycle assessment: a bibliometric analysis. *International Journal of Life Cycle Assessment, 20,* 541–555. http://dx.doi.org/10.1007/s11367-015-0846-2

İleri, Y. Y. & Kara, B. (2022). Covid-19 pandemi sürecinde kullanılan güncel sağlık bilişim uygulamaları ve yenilikçi teknolojiler: insanlığa katkıları ve temel kaygılar. *Sağlık ve Toplum, 32*(1), 33–52. https://l24.im/FphtX

İleri, Y. Y. (2018). *Sağlık yönetim bilişim sistemleri.* Çizgi Kitabevi.

Karaarslan, E., Ergin, A. M., Turğut, N. & Kılıç, Ö. (2015, Aralık 1-3). Elektronik sağlık kayıtlarının gizlilik ve mahremiyeti [Konferans Sunumu]. İnet-Tr'15, XX. Türkiye'de İnternet Konferansı, İstanbul, Türkiye. http://inet-tr.org.tr/inetconf20/kitap/inet15-EKaraarslan-AMErgin-NTurgut-OKilic.pdf

Kılcan, B. & Gülbudak, B. (2019). E-Okuryazarlığa Yönelik Tutum Ölçeğinin Geliştirilmesi: Geçerlik ve Güvenirlik Çalışmaları. *Ahmet Keleşoğlu Eğitim Fakültesi Dergisi (AKEF), 1*(1), 59-71. https://doi.org/10.38151/akef.573786

Kişisel Verileri Koruma Kurumu. (t.y.). Kamuoyu duyurusu (veri ihlali bildirimi) – Beytıp Sağlık Hizmetleri Ltd. Şti. https://www.kvkk.gov.tr/Icerik/7556/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Beytip-Saglik-Hizmetleri-Ltd-Sti-

Koppel, R. (2012). Patient safety and health information technology: learning from our mistakes. https://psnet.ahrq.gov/perspective/patient-safety-and-health-information-technology-learning-our-mistakes

Li, M., Lou, W. & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless Communications, 17*(1), 51–58. http://dx.doi.org/10.1109/MWC.2010.5416350

Lundgren B. & Möller N. (2019). Defining information security. *Science and Engineering Ethics, 25,* 419–441. https://doi.org/10.1007/s11948-017-9992-1

Luxton, D. D., Kayl, R. A. & Mishkind, M. C. (2012). mHealth data security: the need for hipaa-compliant standardization. *Telemedicine and e-Health, 18*(4), 284-288. https://doi.org/10.1089/tmj.2011.0180

Martínez, M. A., Cobo, M. J., Herrera, M. & Herrera-Viedma, E. (2015). Analyzing the scientific evolution of social work using science mapping. *Research on Social Work Practice, 25*(2), 257–277. https://doi.org/10.1177/1049731514522101

Martín-Martín, A., Thelwall, M., Orduna-Malea, E. & Delgado López-Cózar. (2021). E. Google scholar, microsoft academic, scopus, dimensions, web of science, and opencitations' cocı: a multidisciplinary comparison of coverage via citations. *Scientometrics, 126,* 871-906. https://doi.org/10.1007/s11192-020-03690-4

Moody, G. D., Siponen, M. & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly: Management Information Systems, 42*(1), 285–311. https://misq.umn.edu/skin/frontend/default/misq/pdf/appendices/2018/V42I1Appendices/14_13853_RA_MoodyAppendices.pdf

Peikari, H. R., Ramayah, T., Shah, M. H. & Lo. M. C. (2018). Patients' perception of the information security management in health centers: the role of organizational and human factors. *BMC Medical Informatics and Decision Making, 18,* 102. https://doi.org/10.1186/s12911-018-0681-z

Pfleeger, S. L. & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611. https://doi.org/10.1016/j.cose.2011.12.010

Polat, Z. A., Saraçoğlu, A. & Duman, H. (2019). Harita dergisi'nin bibliyometrik analizi. *Harita Dergisi, 161,* 46–56. https://www.harita.gov.tr/uploads/files/articles/harita-dergisinin-bibliyometrik-analizi-1191.pdf

Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S. & Aji, R. F. (2022). Information security behavior in health information systems: a review of research trends and antecedent factors. *Healthcare (Switzerland), 10*(12), 2531. https://doi.org/10.3390/healthcare10122531

Silomon, J. (2020, September 30). The Düsseldorf cyber incident. https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident

Smart, W. (2018). Lessons learned review of the WannaCry Ransomware Cyber Attack. United Kingdom Department of Health and Social Care. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

SPIEGEL Netzwelt. (2020, September 17). Ermittlungen wegen fahrlässiger Tötung eingeleitet. https://l24.im/87V0Fbu

T.C. Kalkınma Bakanlığı. (2018). *On Birinci Kalkınma Planı (2019-2023) Bilgi ve İletişim Teknolojileri Özel İhtisas Komisyonu Raporu.* T.C. Kalkınma Bakanlığı. https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf

Tidy, J. (2020, September 18). Police launch homicide inquiry after German hospital hack. https://www.bbc.com/news/technology-54204356

Tsohou, A., Karyda, M. & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & Security, 52,* 128-141. https://doi.org/10.1016/j.cose.2015.04.006

Ture, N., Tunc, Y. & Aksoy, C. (2022). Awareness Among Otorhinolaryngologists of Literature Resources: Survey Research. *Selcuk Medical Journal, 38*(3), 114-120. https://dx.doi.org/10.30733/std.2022.01561

Universitätsklinikum Düsseldorf. (2020a, September 10). Krankenhaus derzeit nur sehr eingeschränkt erreichbar – Patientenversorgung eingeschränkt. https://l24.im/NDdyQ

Universitätsklinikum Düsseldorf. (2020b, September 11). Update 16 Uhr - Uniklinik Düsseldorf: Massiver Netzwerkausfall. https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/update-16-uhr-uniklinik-duesseldorf-massiver-netzwerkausfall

Universitätsklinikum Düsseldorf. (2020c, September 14). Update 14.9. / 13:30 Uhr - Uniklinik Düsseldorf: IT-Ausfall hält an. https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/update-149-1330-uhr-uniklinik-duesseldorf-it-ausfall-haelt-an

Universitätsklinikum Düsseldorf. (2020d, September 17). IT-Ausfall an der Uniklinik Düsseldorf. https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/it-ausfall-an-der-uniklinik-duesseldorf

Universitätsklinikum Düsseldorf. (2020e, September 18). Update 18.9.–IT-Ausfall an der Uniklinik Düsseldorf. https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/update-189-it-ausfall-an-der-uniklinik-duesseldorf

Universitätsklinikum Düsseldorf. (2020f, September 23). Uniklinik Düsseldorf wieder bereit für Notfälle. Universitätsklinikum Düsseldorf. https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/uniklinik-duesseldorf-wieder-bereit-fuer-notfaelle

Universitätsklinikum Düsseldorf. (2020g, October 12). Wieder normale Patientenzahlen nach IT-Ausfall. Universitätsklinikum Düsseldorf. https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/wieder-normale-patientenzahlen-nach-it-ausfall

van Eck, N. J. & Waltman, L. (2010). Software survey: vosviewer, a computer program for bibliometric mapping. *Scientometrics, 84,* 523–538. https://doi.org/10.1007/s11192-009-0146-3

Varol, Ş., Orhan, F., Tuncer, S. & Akyüz, S. (2016). Sağlık kurumlarında bilgi güvenliği bağlamında biyometrik sistemler. *Sağlık Akademisyenleri Dergisi, 3*(4), 155–162. https://dergipark.org.tr/tr/pub/sagakaderg/issue/46735/586227

Yeng, P. K., Fauzi, M. A., Sun, L. & Yang, B. (2022). Assessing the legal aspects of information security requirements for health care in 3 countries: scoping review and framework development. *JMIR Human Factors. 2022; 9*(2), e30050. https://doi.org/10.2196/30050

Yıldız, B. & Gejam, E. H. Y. (2022). Cyber-physical systems and cyber security: a bibliometric analysis. *OPUS Journal of Society Research, 19*(45), 35–49. https://doi.org/10.26466/opusjsr.1063227

Zupic, I. & Čater, T. (2015). Bibliometric methods in management and organization. *Organizational Research Methods, 18*(3), 429–472. https://doi.org/10.1177/1094428114562629

Wilkowska, W. & Ziefle, M. (2012). Privacy and data security in e-health: requirements from the user's perspective. *Health Informatics Journal, 18*(3), 191-201. https://doi.org/10.1177/1460458212442933

## EXTENDED ABSTRACT

**Introduction:** Ensuring information security in healthcare is of paramount importance due to its sensitive nature (Deniz, 2023). A study conducted with healthcare professionals regarding information security, revealed that while healthcare professionals make efforts to prioritize information security, they struggle to maintain it at an adequate level (Baran and Şener, 2019). Another study suggests that healthcare professionals are increasingly becoming more aware of information privacy during their undergraduate education, underlining the growing significant of this aspect (Bahar et al., 2022). Consequently, potential information security breaches within healthcare institutions carry severe repercussion, including financial loses, data breaches and in extreme cases, patient fatalities. In light of these concers, it is imperative to conduct further research and implement measures that address information security in health institutions.

**Method:** In this bibliometric study, the objective is to assess the existing literature pertaining to "information security management in health institutions". The aim is to identify fundamental relationship networks and focal area of research within this domain, threby providing a scholary foundation for future researches in these field. The research utilized Web of Science (WoS) as the primary database fort he review. Data extraction from the WoS Core Collection was conducted on May 28, 2023. Title search, where keywords such as "information security", "data security", "cyber security" and "cybersecurity" were inputted. Subsequently, a second search was conducted encompassing keywords like "health", "healthcare", "health care", "hospital", "health institutions", "health care institutions", "clinic", "health centre", "health home", "dialysis centre", "birthing centre" and "urgent care centre". These searches were performed across all fields to comprehensively capture relevant publication.

**Results:** The total number of citations for analyzed literature is 5,194, with an average of 123.66 citation per year. Notably, the concentration of both citations and publications is primarily observed within the last six-year, spanning from 2018 to May – 28, 2023. This period account for 82.69% (4,295) of the total citations and 69.78% (260) of the total publications. Consequently, when evaluating this spesific time frame, the average number of citations over the last six years amounts to 1,369, while the average number of publications is 74. An additional aspect worth considering in the analysis of citation is the present of self-citations. As indicated by WoS Citation Report, self-citations constitute a modest is 3.25% (169) of the overall citation count. This relatively low rate of self-citation can be interpreted as a positive indicator fort he field, reflecting a reduced likelihood of biased or insular referencing practices. The top ten journals with the highest number of publications account for 18.51% of the total number of publications in this field, which corresponds to 70 publications (n=70). Notably, the first three journals within this group make up a substantial 50% of the top ten, with 35 publications (n=35) When these journals are categorized according to the WoS Journal Citation Report (JCR) classification, it becomed evident that the publications are predominantly concentrated in the areas of health informatics and computer science-information systems. "IEEE" and "Elsevier" emerge as prominent publishers in this fieldi with IEEE apearing to hold a competitive advantage. Notably, two different journals affiliated with IEEE, despite having only one publication each, rank as the second and third most cited in the field. This trend is also reflected in terms of impact rate. IEEE boasts an impressive 60.78 impact rate across four journals, whereas Elsevier maintains a 25.55 impact rate with three journals. Moreover, it's worth mentioning that the most cited publication in the field is "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Priacy?" authored by Esposito et al (2018). In 2018. This publication has garnered significant attention and citation within the field, underlining the importance of the topic it addresses.

**Discussion:** Regarding the distribution of journals in the field, IEEE published journals emerge as a leading presence. IEEE enjoys a robust position, excelling the both the quantity of publications and the number of citations. The effectiveness of IEEE's journals is widely acknowledged in the field, and it is anticipated that researchers embarking on new studies in this area will prominantly consider IEEE as their primary journal choice. Furthermore, a noteworthy aspect for discussion within this study pertains to the current state of keyword usage. As illustrated in Table 9, variations exist in the utilization of keywords by researchers in the field. These discrepancies warrant further exploration and analysis,

underscoring the evolving landscape of terminology and focus within the research domain. These variation exhibit remarkable similarities, such as “health care”-“healthcare”, “information security”-“information security” or “iot”-“iomt”. Consequently, it is evident that there researcher tend to exhibit a terminological consistency in their keyword preferences. In this respect, it reveals the importance of the use of standardisation studies in order to ensure terminological commonality. This underscores the significance of standartization efforts to establish a common terminology, highlighting the need for initiatives that promote terminological uniformity within the field.

**Conclusion and Suggestions:** This study sought to provide an overview of the academic research landscape pertaining to “information security in healthcare institutions” and to offer evaluations based on the findings. The field exhibits a trajectory that align closely with technological advancement, but its growth has been relatively recent due to contexual factors. As a result of this examination, it becomes apparent that there is a need for more extensive and comprehensive research endeavors that address not only the technical aspects of information security in healthcare but also its legal, ethical, and organizational dimensions. These encompass elements like legal compliance, ethical considerations and organizational factors such as personnel perception and digital literacy. Such multifaceted investigations are likely to make meaningful contributions to the field, providing a more holistic understanding of information security in healthcare.