Araştırma Makalesi

E-İmza Güvenliğine Yönelik Bir Araştırma: Bibliyometrik Bir Analiz

A Research on E-Signature Security: A Bibliometric Analysis

Nilhan Köksal*, Eyüp Burak Ceyhan**

*Sorumlu yazar, Bartın Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilişim Sistemleri ve Teknolojisi ABD., Bartın, Türkiye. E-posta: nilhan.koksal@hotmail.com
Bartın University, Graduate School, Department of Information Systems and Technologies, Bartın, Türkiye. E-mail: nilhan.koksal@hotmail.com
** Doç. Dr., Bartın Üniversitesi Mühendislik Mimarlık ve Tasarım Fakültesi, Bilgisayar Mühendisliği, Bartın, Türkiye. E-posta: mailto:eyupburak@gmail.com
Bartın University, Faculty of Engineering, Architecture and Design, Department of Computer Engineering, Bartın, Türkiye. E-mail: eyupburak@gmail.com

Atıf: Köksal, N., & Ceyhan, E.B. (2026). E-imza Güvenliğine Yönelik Yapılan Araştırmaların Bibliyometrik Analizi. *Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *17*(1), 49-64. https://doi.org/10.47129/bartiniibf.1801203

Makale Bilgisi

Makale Tarihçesi
Geliş Tarihi:
10.10.2025
Kabul Tarihi:
06.01.2026
Yayımlanma Tarihi:
31.05.2026

Anahtar Sözcükler
E-İmza
Elektronik Imza
Güvenlik
Kimlik Doğrulama
Blokzincir

JEL Kodları
D81, D82, L86

Öz

Amaç: *Bu çalışmada e-imza güvenliğine yönelik yapılan araştırmaların bibliyometrik analizinin yapılması amaçlanmıştır.*

Yöntem: *Çalışmada Scopus veri tabanında 1979–2024 yılları arasında, başlık, özet ve anahtar kelime alanlarında "security" ve "electronic signature" terimleri AND operatörü kullanılarak aranmış; dil ve belge türü açısından herhangi bir sınırlama yapılmaksızın toplam 487 dokümana ulaşılmıştır. Elde edilen veriler VOSviewer programı aracılığıyla bibliyometrik analiz yöntemi kullanılarak incelenmiştir. Gerçekleştirilen analiz kapsamında ortak yazarlık analizi, yazar atıf analizi, anahtar sözcük analizi ile yazarların bağlı oldukları kurumlar ve ülkeler değerlendirilmiştir.*

Bulgular: *Çalışma sonucunda analiz yapılan konuda yeterli sayıda yayın olmadığı belirlenmiştir. En çok atıf alan yazarlar incelendiğinde, Mangard S., Oswald S. ve Popp T.'nin 1770 atıf ile en yüksek değere sahip oldukları ve diğer yazarlara göre belirgin biçimde daha fazla atıf aldıkları saptanmıştır. Anahtar sözcük analizi sonuçlarına göre literatürün büyük oranda "e-imza", "güvenlik", "elektronik imza" ve "kimlik doğrulama" kelimelerinde yoğunlaşmaktadır. Yapılan yayınların ülke bazlı analiz sonuçlarına göre e-imza güvenliği alanında en fazla yayın üreten ülkelerin sırasıyla Amerika Birleşik Devletleri, Çin, Avusturya ve Almanya olduğu tespit edilmiştir.*

Sonuç: *E-imza güvenliği alanındaki çalışmaların sınırlı sayıda olduğu ancak giderek teknolojik çeşitlilik kazandığı görülmektedir. Araştırmaların özellikle gelişmiş kriptografik algoritmalar, blokzincir tabanlı güvenlik modelleri, kuantum bilişim odaklı imza protokolleri ve yapay zekâ temelli doğrulama sistemleri doğrultusunda şekillendiği değerlendirilmektedir. Bu durum, alanın disiplinler arası ve yenilikçi araştırmalara açık olduğunu göstermektedir.*

Article Information

Article History

Received:
10.10.2025
Accepted:
01.06.2026
Published:
05.31.2026

Keywords

E-Signature
Electronic Signature
Security
Authentication
Blockchain

JEL Codes

D81, D82, L86

Abstract

Purpose: *This study aims to conduct a bibliometric analysis of research on e-signature security.*

Method: *In this study, the Scopus database was searched for the terms "security" and "electronic signature" in the title, abstract, and keyword fields covering the years 1979–2024. A total of 487 documents were retrieved without any restrictions on language or document type. The data obtained were analyzed using the bibliometric analysis method through the VOSviewer software. The analysis included co-authorship analysis, author citation analysis, keyword analysis, as well as the examination of authors' affiliated institutions and countries.*

Findings: *The results indicate that the number of publications in the analyzed field is limited. Citation analysis revealed that Mangard S., Oswald S., and Popp T. share the highest citation count with 1,770 citations each, significantly exceeding other authors. Keyword analysis showed that the literature largely concentrates on "e-signature," "security," "electronic signature," and "authentication." Country-based analysis demonstrated that the United States, China, Austria, and Germany are the leading countries in terms of publication output in the field of e-signature security.*

Conclusion: *Although the number of studies on e-signature security is limited, the field has been gaining technological diversity. Research trends indicate a focus on advanced cryptographic algorithms, blockchain-based security models, quantum computing-oriented signature protocols, and artificial intelligence-based verification systems. These findings suggest that the field is open to interdisciplinary and innovative research developments.*

Giriş

İmza, hukuksal olarak geçerli olup kişinin iradeli olarak bir işlemi onayladığı anlamına gelmektedir. Somut olarak atılan fiziksel imzanın, bir başka deyişle geleneksel imzanın dışında bilişim teknolojileri dünyasında elektronik imza (e-imza) bulunmaktadır. Soyut olan elektronik imzanın da fiziksel imzada olduğu gibi kişinin önüne sunulan belge veya görüşü onayladığı kabul edilmektedir (León, 2023). Elektronik imzaların bazı riskleri vardır. Bu riskler arasında izinsiz olarak alınabilmesi ve kötü amaçlarla kullanılabilmesi yer almaktadır. Bu sorunları çözmek için imza tanıma teknolojilerinin geliştirilmesi gibi konuyla ilgili birçok çalışma yapılmaktadır (Wang, 2024).

Dünyada elektronik imza uygulamalarının, e-devlet, vergi ve bankacılık işlemlerinde yaygın olarak kullanıldığı görülmektedir. Ülkemizde ise bu alandaki ilk uygulama dış ticaret alanında olmuştur (Bengshir & Topcan, 2008). Türkiye'de e-imzanın hukuki altyapısının oluşturulması, Dış Ticaret Müsteşarlığı ve Elektronik Ticaretin Geliştirilmesi Konseyi iş birliğinde başlatılmıştır. Elektronik İmza Kanunu Tasarısı 2004 yılında kanunla yürürlüğe girmiştir (Sağiroğlu & Alkan, 2005).

Ülkemizde e-imzanın en çok kullanıldığı alanlardan biri de sağlık hizmetleridir. E-imza'nın sağlık alanında kullanılmasıyla birlikte kişilerin özellikle reçetelerinin ve

tedavi işlemlerinin daha hızlı onaylanması sağlanmaktadır. Bu durum sağlık hizmeti alan kişiler için zaman tasarrufu sağlamaktadır (Çoban, 2023). Ayrıca verimliliğin artmasıyla birlikte giderler de azalmaktadır. E-imza ile iş yaşamında ortaklık ve anlaşmaların hızlanması sağlanmıştır. E-imza hukuki olarak geçerlidir fakat iş hayatında dijital teknolojilere karşı güven problemi bulunduğundan dolayı çoğunlukla somut nesnelerle işlemler tercih edilmektedir. Bu problemin bir diğer nedeni kullanıcıların ve şirketlerin dijitalleşmeye geçiş sürecinde yaşadığı sıkıntılardır. Veri güvenliğindeki kurallar, teknoloji kullanımına dair bilgi ve becerilerin yetersizliği, küçük ve orta ölçekli işletmelerin teknoloji dünyasına henüz tam olarak entegre olamamaları problemler arasında yer almaktadır (Borcoşi vd., 2023).

Nitekim, e-imzanın kör imza, tuzak imza, vekâlet imzası, inkâr edilemeyen imza şeklinde türleri bulunmaktadır. Kör imza bir kimsenin, belgeyi içeriğini görmeden imzalamasıdır. Riskli sonuçlar doğurabilir. Tuzak imza sahte imzanın sahte olduğunu kanıtlamaya yarayan protokoldür. Vekâlet imzası bir kişinin imzasını, gizli anahtarını açmadan başka birine kullandırma hakkı tanır. İnkâr edilemeyen imza imzalayan kişinin rızası olmadan doğruluğu kanıtlanamayan dijital imza protokolüdür (Güler & Ömürgönülşen, 2011).

Bu çalışmada e-imza güvenliğine yönelik yapılan araştırmaların bibliyometrik analizinin yapılması amaçlanmıştır. Çalışmanın akışında öncelikle konuyla ilgili literatür taraması verilecek, ardından araştırmanın yöntemi tanıtılacaktır. Sonrasında uygulama bulguları verilerek sonuç ve önerilerde bulunulacaktır.

Literatür Taraması

E-imza güvenliği üzerine yapılan literatür çalışmalarında, farklı güvenlik protokollerinin ve büyümelerinin etkili bir şekilde uygulanabileceği çeşitli yöntemler üzerinde durulmuştur. E-imza sistemleri, dijital imzaların doğruluğunu ve güvenliğini sağlamak amacıyla kullanılan bir yöntem olarak son yıllarda önemli bir araştırma konusu haline gelmiştir. Yapılan literatür taramalarında, e-imza güvenliğine dair daha önce bibliyometrik çalışmanın yapılmadığı tespit edilmiştir. Bu durum, e-imza güvenliği alanında mevcut araştırmaların içerik yönünden zengin olmasına karşın, genel eğilimlerin ve araştırma yönelimlerinin sistematik biçimde incelenmediğini göstermektedir.

Elektronik imzalar, e-devlet hizmetleri veya e-bankacılık gibi güvenlik açısından hassas uygulamalarda yaygın olarak tercih edilmektedir. Bu tarz dijital imzalar, işlemlerin doğruluğunu ve güvenliğini sağlamak amacıyla kullanılmaktadır (Zefferer, 2014). Bu kapsamda, e-imza güvenliğini sağlamaya yönelik farklı teknolojik yaklaşımlar da literatürde ön plana çıkmaktadır.

E-imza güvenliğinde kullanılan teknolojilerden biri blokzincirdir. Son yıllarda güvenli dijital doğrulama süreçlerinde en çok tartışılan yeniliklerden biri blokzincir teknolojisidir. Djajadi vd., (2023) blokzincir tabanlı bir e-sertifika sistemi ve otomasyon sistemi önererek, dijital nesne sahtekarlığını önlemeyi sağlamaktadır. Fang vd., (2020) tarafından yapılan bir araştırmada, blokzincir teknolojisinin merkezi otoriteye ihtiyaç

duymayan yapısının yanı sıra güvenlik ve doğrulanabilirlik açısından dijital imzaların önemli olduğu vurgulanmaktadır. Araştırmada farklı dijital imza yöntemleri sınıflandırılmış, güvenlik ve performans bakımından analiz edilerek gelecekte daha verimli imza algoritmalarının tasarlanmasına yönelik öneriler sunulmuştur. Bu bağlamda literatürde blokzincir temelli e-imzalar yalnız veri bütünlüğü değil, aynı zamanda işlemlerin değiştirilemez olduğunu göstermekte, dolayısıyla e-imza güvenliği araştırmalarında blokzincir destekli çözümlerin ön plana çıkmasına katkı sunmaktadır. Haikal & Mahmudah (2024) tarafından yapılan bir araştırmada, elektronik imzaların e-devlet uygulamalarında avantajlarını, kullanımını ve karşılaşılan engelleri incelemiştir. Çalışma, blokzincir teknolojisinin elektronik imzalarla entegrasyonunun, güvenliği artırabileceğini ve işlemlerin şeffaflığını sağlayabileceğini belirtmektedir. Ancak, bu entegrasyonun teknik zorluklar ve yasal engellerle karşılaştığını belirtmektedir. Elektronik imzaların uluslararası geçerliliği, farklı ülkelerdeki yasal çerçevelerin çeşitliliği nedeniyle literatürde önemli bir konu olarak yer almaktadır. Örneğin Zhang vd., (2021) çalışmasında, farklı ülkelerdeki e-imza yasalarını karşılaştırmış ve uluslararası uyumsuzlukları analiz etmişlerdir. Çalışma, Avrupa Birliği'nde eIDAS Yönetmeliği ve Amerika Birleşik Devletleri'ndeki ESIGN ve UETA yasalarının, e-imzaların yasal geçerliliğini sağlamak amacıyla çeşitli yaklaşımlar göstermektedir. Söz konusu çeşitlilikler, küresel ölçekte e-imza uygulamalarının uyumluluğunu zorlaştırmakta ve hukuki belirsizlikler doğurmaktadır. Bu durum, uluslararası e-imza uygulamalarında ortak standartlar ve uyumun önemini ortaya koymaktadır (Zhang vd., 2021).

Blokzincir tabanlı sistemlere ek olarak, geleceğe dönük güvenlik tehditleri açısından kuantum bilişim yaklaşımları da dikkat çekmektedir. Literatürde, kuantum bilişim alanında da var olan kriptografik yapılar üzerinde oluşturabileceği risklere karşı, kuantum dijital imza tabanlı blokzincir algoritmalarının geliştirildiği görülmektedir. Bu yaklaşımlar, e-imza güvenliğinin gelecekteki altyapısına yön verebilecek nitelikte olduğunu göstermektedir (Wang vd., 2022). Ayrıca genelleştirilmiş kuantum destekli dijital imza (GQaDS) şeması, kuantum anahtar dağıtımı kullanarak dijital imzaların güvenliğini artırmakta sahteciliğe karşı korumayı güçlendirmekte ve imza uzunluğunu azaltmaktadır (Tarable vd., 2025).

Blokzincir teknolojisinin uygulanabilirliğini gösteren bir diğer örnek, sağlık sektöründe görülmektedir. Pandemi döneminde kullanılan elektronik aşı sertifikasında gizlilik sağlamak amacıyla blokzincir teknolojisiyle birlikte kriptografi kullanılmıştır. Toubiana vd., (2022) yaptıkları çalışmada blokzincir teknolojisi kullanılarak hastanın elektronik aşı sertifikasına ulaşılabilmesi sağlanmıştır.

Benzer şekilde, finans alanında da blokzincir destekli e-imza uygulamaları yaygınlaşmaktadır. Blokzincir teknolojisinin kullanıldığı sistemlerden biri de elektronik çektir. Elektronik imza uygulamalarıyla bağlantılı olarak elektronik çek uygulaması yeni bir teknolojidir ve geleneksel çek sistemlerinin yerine kullanılmaktadır. Dünyada kullanılan bu elektronik onaylama ve imza yöntemleri giderek yaygınlaşmaktadır (Ber, 2022).

Kriptografi ve blokzincir tabanlı çözümlerin yanı sıra, geleneksel imza güvenliğini artırmaya yönelik farklı teknolojik yaklaşımlar da geliştirilmiştir. Literatürde geleneksel imza güvenliği ile ilgili güvenlik problemlerini giderebilmek için çalışmalar yapıldığı görülmüştür. Sahte imzaları anlamak için makine öğrenimi yaklaşımları ve yapay zekâ desteği kullanılmaktadır. Örneğin Jadhav vd., (2025), yaptıkları çalışmada makine öğrenimi ve görüntü işleme yöntemleri ile imza doğrulama sistemi geliştirildiğini ve yüksek doğrulukla imzaların ayrıştırıldığını savunmaktadır.

Literatürde elektronik imza ve güvenliği konusuna yönelik çok sayıda teknik, hukuki ve uygulamalı çalışma bulunmasına rağmen, bu çalışmaların genel eğilimlerini, araştırma yönelimlerini ve iş birliği ağlarını sistematik biçimde ortaya koyan bibliyometrik analizlerin oldukça sınırlı olduğu görülmektedir. Mevcut çalışmalar çoğunlukla belirli bir teknolojiye, ülkeye veya uygulama alanına odaklanmakta; alanın bütüncül gelişimini ve araştırma dinamiklerini kapsamlı biçimde değerlendirmemektedir. Bu durum, e-imza güvenliği alanındaki araştırmaların hangi temalar etrafında yoğunlaştığı, hangi teknolojilerin ön plana çıktığı ve hangi konuların ihmal edildiği konusunda genel bir çerçevenin eksik kalmasına neden olmaktadır. Bu çalışmada gerçekleştirilen bibliyometrik analiz, söz konusu boşluğu doldurmayı amaçlayarak e-imza güvenliği literatürünün yapısal özelliklerini, tematik eğilimlerini ve gelecekteki araştırma yönelimlerini ortaya koymayı hedeflemektedir.

Yöntem

Bibliyometrik analiz; elde edilen belgelerin veya makalelerin belirli özelliklerine göre analiz edilmesi ve bulguların ortaya çıkarılmasına dayanmaktadır. Herhangi bir temaya ait çalışmalar veya bir dergide yayınlanan araştırmalar, farklı parametrelere göre incelenmekte ve bu parametrelere göre bulguların gösterimi sağlanmaktadır. Bu bulgular, atıf, araştırma konusu, yazar sayısı, anahtar kelimeler gibi verileri içerir. Bibliyometrik analizlerde; öğeler arasındaki ilişkilerin araştırılmasında mesafe tabanlı haritalar ve grafik tabanlı haritalardan yararlanılabilmektedir (Artsın, 2020). Metin analizi yapmak için kullanılan programlardan biri de VOSviewer programıdır.

VOSviewer programında seçilen makaleler istenilen özelliklere göre listelenir ve verilerin ilişkileri ortaya çıkar. VOSviewer, araştırma konularının bibliyometrik analizini, temaların ve anahtar kelimelerin oranlarını belirlemeyi, web sayfalarının içerik analizini, öğrenci başarılarının ve tezlerin analizini ve ortak yazarlık ilişkilerini incelemeyi sağlayan bir yazılımdır. Bu program, akademik çalışmalar arasındaki bağlantıları ve eğilimleri keşfetmek için kullanılarak, araştırma verilerini görselleştirme ve analiz etme imkânı sunar (Artsın, 2020).

Araştırmamızda VOSviewer programı ile aşağıdaki parametreler analiz edilmiştir:

- Ortak yazarlık analizi,
- Yazar atıf analizi,
- Anahtar sözcük analizi,

- Yazarların kuruluş yerleri,
- Yazarların ülkeleri.

Elektronik imza güvenliği ile ilgili bu bibliyometrik analiz çalışmasında VOSviewer programı kullanılmıştır. Dokümanlar Scopus üzerinden indirilmiştir. Scopus'ta "security" ve "electronic signature" kelimeleri aratılarak 487 adet dokümana ulaşılmıştır. Arama yapılırken kullanılan kriterler Tablo 1'de verilmiştir. Bu çalışmada kullanılan bibliyometrik veriler, Scopus veri tabanından Ekim 2024 tarihinde indirilmiştir. Veri seti oluşturulurken yinelenen kayıtlar kontrol edilmiş ve analiz sürecinden çıkarılmıştır. Bibliyometrik analizlerde kullanılan yayınlar ve atıflar, analiz türüne göre belirlenmiş olup, ağ haritalarının anlamlı ve okunabilir olması amacıyla düşük frekanslı öğeler analiz dışı bırakılmıştır. Analizler, VOSviewer yazılımı kullanılarak gerçekleştirilmiş ve ağ haritalarının oluşturulmasında association strength normalizasyon yöntemi tercih edilmiştir. Bu yöntem, öğeler arasındaki ilişkilerin daha dengeli ve karşılaştırılabilir biçimde görselleştirilmesini sağlamaktadır.

Tablo 1: *Arama Kriterleri*

Veri Tabanı	Scopus
Tarih Aralığı	1979-2024
Aranan Yer	Başlık, özet, anahtar kelime
Aranan Kelimeler	"security", "electronic signature"
Operatör	AND
Belge Türü	Tüm
Dil	Hepsi

Kaynak: Yazarlar tarafından oluşturulmuştur.

Bulgular

Çalışmada VOSviewer programında Scopus'tan elde edilen veriler analiz edilmiştir. Elde edilen bulgular bu bölümde sunulmuştur.

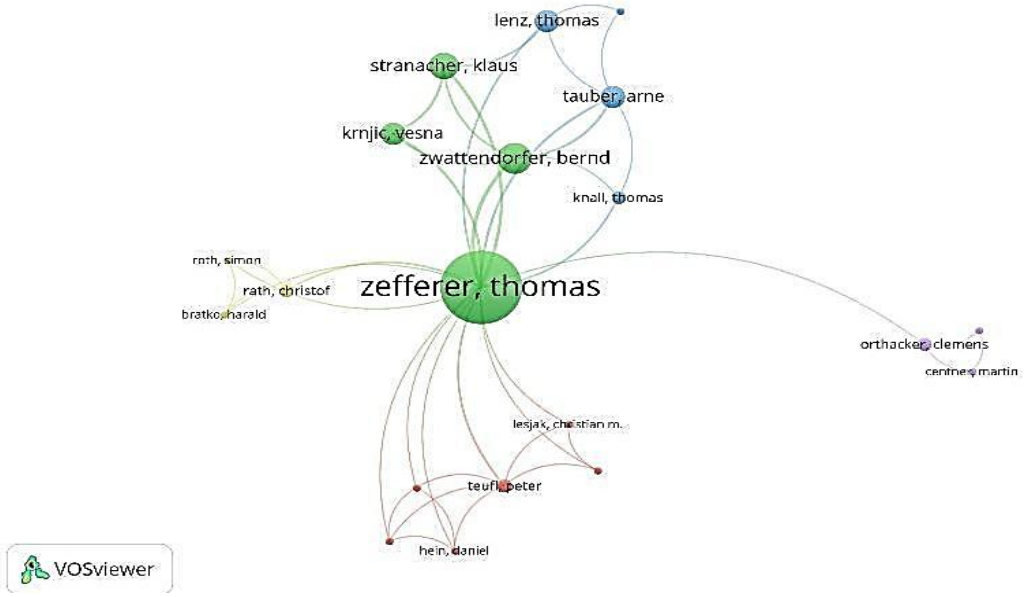
Yapılan ortak yazarlık analizi sonucunda en çok üretkenlik gösteren ilk on yazar ve bu yazarlara ait yayın sayısı Tablo 2'de sunulmuştur. Yazarlar arasındaki ilişki analizi ise Şekil 1'de gösterilmiştir.

Tablo 2: *En Çok Üretkenlik Gösteren Yazarlar*

Yazar	Yayın Sayıları
Zefferer T.	18
Zwattendorfer B.	6
Kutylowski M.	6
Stranacher K.	5
Posch,R	5
Allaert, F.Ç.	4
Quantin, C.	4
Tauber, A.	4
Krnjic, V.	4
Tahat, N.	4
Lenz T.	4
Smejkal V.	4
Struif B.	4
Srivastava A.	4

Kaynak: Yazarlar tarafından oluşturulmuştur.

Tablo 2 ve Şekil 1 incelendiğinde bu konuda en fazla yayın yapan yazarların bile kısıtlı sayıda yayın yaptıkları, yazarların çoğunun ise ortak yayınlarda yazarlık yaptığı görülmektedir. En fazla yayın yapan yazarlar arasında ilk sırada 18 yayın ile Zefferer T. olurken, ikinciliği 6'şar yayınla Zwattendorfer B. ve Kutylowski M. paylaşmıştır. Üçüncü sırayı ise Stranacher K. ve Posch R. paylaşmaktadır.



Şekil 1: *Ortak Yazarlık Analizi*

Kaynak: Yazarlar tarafından oluşturulmuştur.

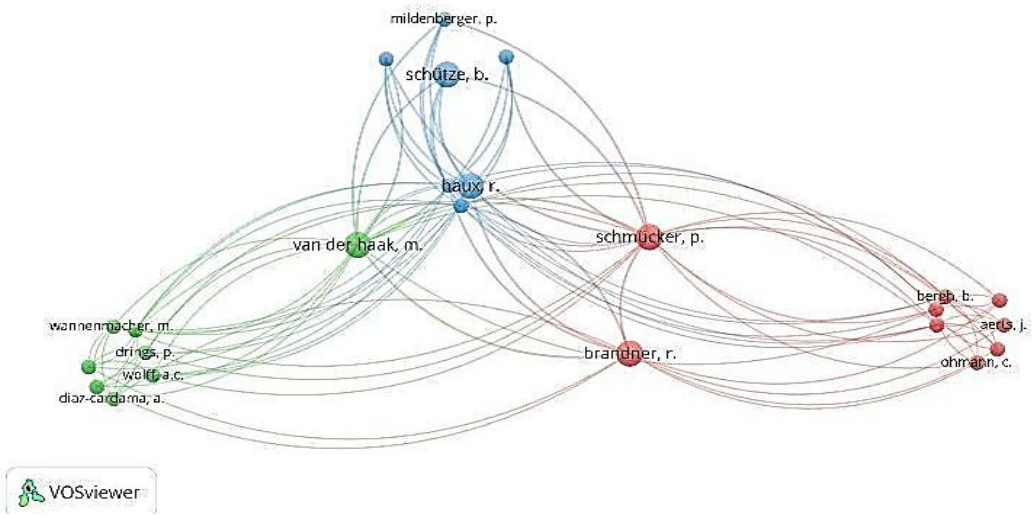
Tablo 2 ve Şekil 1'de yer alan bulgular, yazarların araştırmalarda birbirleriyle ilişkili olduğu görülmektedir. Tablo 2'ye göre, en yüksek üretkenlik gösteren yazarın Zefferer Thomas olduğu görülmektedir. Ayrıca, Şekil 1'de ağ haritası biçiminde oluşturulan analizde, yazarlar arasındaki ortak çalışmalar değerlendirildiğinde, Zefferer Thomas'ın diğer yazarlarla en fazla iş birliği yaptığı tespit edilmiştir. Bu bulgu, söz konusu alanda Zefferer Thomas'ın hem bireysel üretkenliği hem de araştırma iş birlikleri açısından merkezi bir konumda olduğunu ortaya koymaktadır.

Tablo 3: *En Çok Atıf Yapılan Yazarlar*

Yazar	Atıf Sayısı
Mangard S.	1770
Oswald E.	1770
Popp T.	1770
Bernito E.	327
Sandhu R.	327
Van Der Haak M.	99
Baik D-K.	89
Kim Y-G.	89
Lee E.	89
Seo Y-D	89
Seol K.	89

Kaynak: Yazarlar tarafından oluşturulmuştur.

Tablo 3'e göre en çok atıf yapılan yazarlarda ilk üç kişinin atıf sayıları aynıdır. Buna göre; Mangard S., Oswald S., Popp T. 1770 tane atıfla ilk sırayı paylaşmaktadırlar. Bu üç yazara yapılan atıf sayılarının diğer yazarlardan çok daha fazla olduğu dikkat çekmektedir. Bernito E. ve Sandhu R. 327 tane atıfla ikinci sırayı paylaşmaktadırlar. Van Der Haak M. ise 99 tane atıfla üçüncü sırada yer almaktadır.

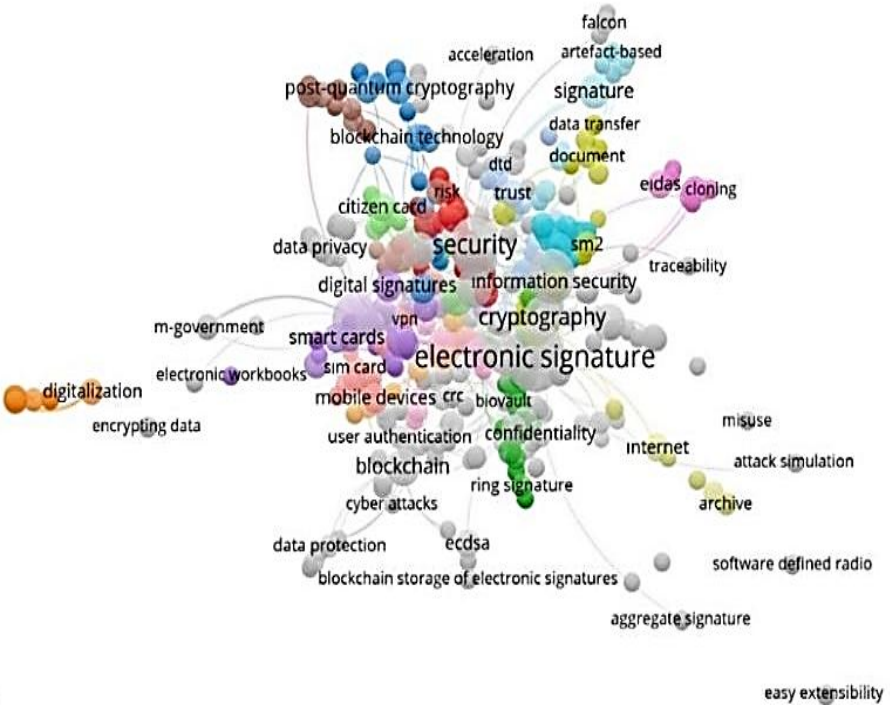


Şekil 2: *Yazar Atıf Analizi*

Kaynak: Yazarlar tarafından oluşturulmuştur.

Şekil 2'de yazarların birbirleriyle atıf ilişkisi ağı görülmektedir. Bu grafiğe göre en çok Haux R.'nin bağlantılı olduğu görülmektedir. En çok atıf yapan yazar Mangard S. iken Haux R.'nin atıf bağlantısının daha çok olduğu görülmektedir.

Yazar atıf analizi sonuçları incelendiğinde, belirli araştırmacıların alandaki bilgi üretimine yön verdiği görülmektedir. Özellikle Mangard S., Oswald E. ve Popp T.'nin yüksek atıf sayılarına sahip olması, bu yazarların e-imza güvenliği ve ilişkili kriptografik yaklaşımlar konusunda temel ve referans niteliğinde çalışmalar ortaya koyduğunu göstermektedir. Buna karşılık, atıf ağında daha fazla bağlantıya sahip olan yazarların, disiplinler arası çalışmalara ve ortak araştırma eğilimlerine daha açık olduğu söylenebilir. Bu durum, e-imza güvenliği alanında bilgi üretiminin belirli çekirdek yazarlar etrafında şekillendiğini ve araştırma iş birliklerinin alanın gelişiminde önemli bir rol oynadığını ortaya koymaktadır.



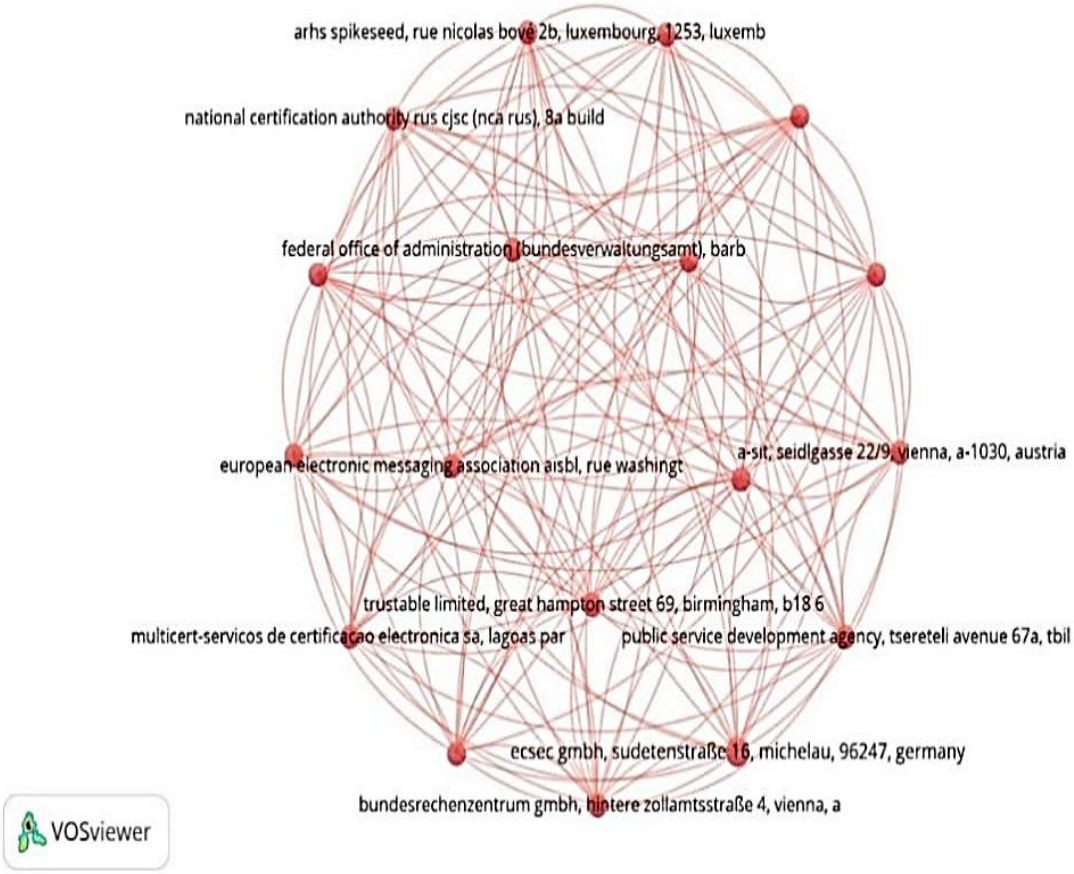
Şekil 3. *Anahtar Sözcük Analizi*

Kaynak: Yazarlar tarafından oluşturulmuştur.

Çalışmalarda yer alan anahtar kelimelerin ilişkisinin analiz edildiği Şekil 3 incelendiğinde, büyük gösterilen anahtar kelimelerin araştırmalarda daha yoğun bir şekilde kullanıldığı görülmektedir. Yapılan bibliyometrik analiz sonucunda, en sık rastlanan sözcüklerin sırasıyla "e-imza", "güvenlik", "elektronik imza", "kimlik doğrulama" ve "kriptografi" olduğu tespit edilmiştir. Bu bulgu, literatürde e-imza güvenliği konusunun temel araştırma alanı olarak ön plana çıktığını göstermektedir. Görsel incelendiğinde, özellikle "e-imza" ve "güvenlik" terimleri üzerine daha yoğun bir odaklanma olduğu, diğer yandan "blokzincir", "dijitalleşme", "kuantum sonrası", "mobil cihazlar", "yüzük imzası" ve "güven" gibi terimlerin daha az sıklıkta yer aldığı

anlaşılmaktadır. Bu durum, e-imza güvenliği literatüründe teknolojik ve yeni gelişen kavramların araştırma yoğunluğunun sınırlı olduğunu ve bu alanlarda daha fazla çalışmaya ihtiyaç bulunduğunu ortaya koymaktadır.

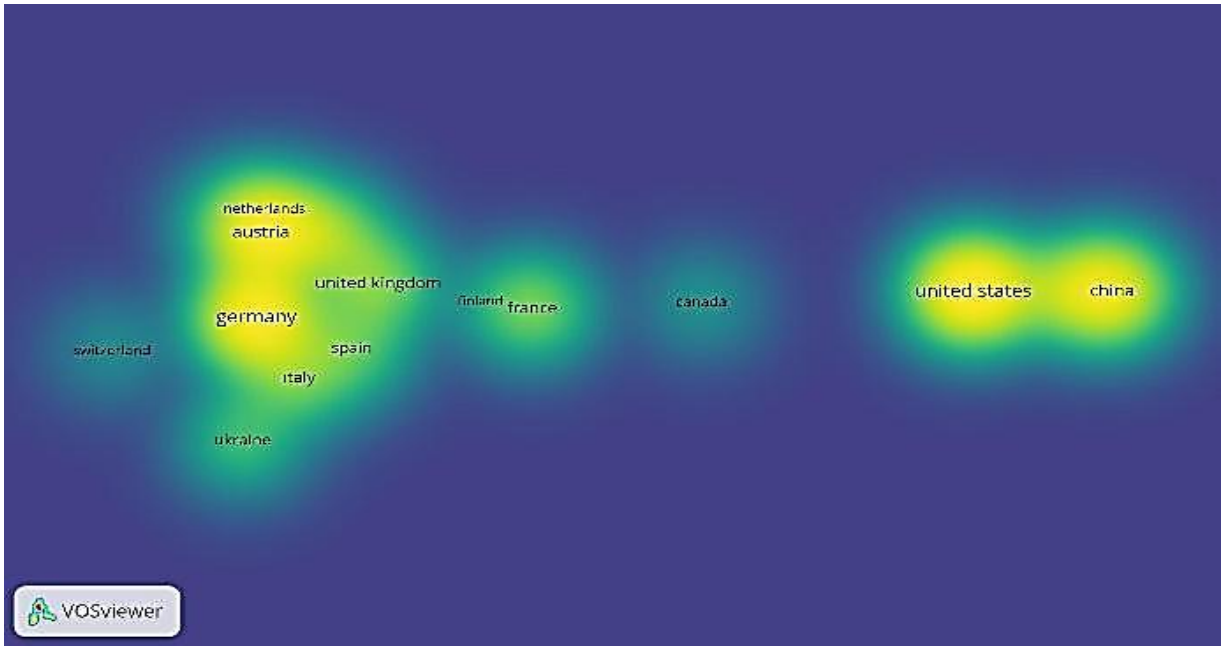
Anahtar sözcük analizi sonuçları, e-imza güvenliği literatürünün büyük ölçüde "e-imza", "güvenlik", "elektronik imza" ve "kimlik doğrulama" kavramları etrafında yoğunlaştığını göstermektedir. Buna karşın "blokzincir", "kuantum sonrası imzalar", "mobil cihazlar" ve "güven" gibi kavramların daha düşük frekansta yer alması, alanın henüz teknolojik olarak olgunlaşma sürecinde olduğunu düşündürmektedir. Bu durum, e-imza güvenliği çalışmalarının ağırlıklı olarak geleneksel kriptografik yaklaşımlara odaklandığını, yeni ve gelişmekte olan teknolojilerin ise literatürde sınırlı düzeyde ele alındığını göstermektedir. Dolayısıyla söz konusu kavramlar, gelecekte yapılacak araştırmalar için önemli potansiyel araştırma alanları olarak değerlendirilebilir.



Şekil 4. *Yazar Kuruluşlarının Görsel Ağ Haritası*

Kaynak: Yazarlar tarafından oluşturulmuştur.

Şekil 4'te e-imza güvenliği üzerine en fazla çalışan kişilerin bulunduğu kuruluşlar gösterilmektedir. Ağ haritasına göre, "Federal office of administration (bundesverwaltungsamt)", "European electronic messaging association aisbl", "national certification authority rus cjsc (nca rus)" dikkat çekmektedir.



Şekil 5. *Yazar Ülkeleri*

Kaynak: Yazarlar tarafından oluşturulmuştur.

Yapılan yayınların ülkeler bazında dağılımı analiz edildiğinde, en yüksek sayıda yayının Amerika Birleşik Devletleri, Çin, Avusturya ve Almanya'da gerçekleştirildiği tespit edilmiştir. Şekil 5 incelendiğinde, bu ülkeleri sırasıyla Fransa, Ukrayna, İngiltere, Finlandiya, İspanya, Kanada ve Hollanda'nın takip ettiği görülmektedir. Analiz, söz konusu ülkelerde e-imza güvenliği alanında gerçekleştirilen çalışmaların diğer ülkelere göre daha yoğun olduğunu göstermektedir.

Genel olarak bulgular, e-imza güvenliği alanında belirli temaların baskın olduğunu, buna karşılık yeni teknolojik yaklaşımların henüz yeterince derinlemesine incelenmediğini ortaya koymaktadır.

Tartışma

Bu araştırmada e-imza güvenliği konusunda literatür incelenerek ve bibliyometrik analiz yapılarak, gelecekte bu alanda çalışma yapmak isteyen araştırmacılara katkı sunulması amaçlanmıştır. Çalışma kapsamında Scopus veri tabanında yer alan 487 çalışma incelenmiştir. Literatürdeki çalışmaların yayın türlerine bakıldığında, araştırmacıların bulgularını daha çok makale veya konferans bildirisi olarak yayımladığı görülmektedir. Bu durum, e-imza güvenliği konusunun son yıllarda hem akademik hem de uygulamalı araştırmalarda ilgi gören bir alan hâline geldiğini göstermektedir.

Bibliyometrik analiz sonuçlarına göre e-imza güvenliği üzerine yapılan çalışmaların tematik olarak daha çok blokzincir, güvenlik, kimlik doğrulama ve kriptografi gibi konularda yoğunlaştığı belirlenmiştir. Anahtar kelime haritalarının incelenmesi, araştırmaların büyük oranda teknik güvenlik mekanizmaları ve kriptografik altyapılar etrafında kümelendiğini ortaya koymuştur. Buna karşılık mobil cihazlar, kuantum

sonrası imzalar, dijitalleşme, yüzük imzası ve güven gibi kavramların literatürde görece az yer aldığı tespit edilmiştir. Bu durum, gelecekteki çalışmalar için bu kavramların derinlemesine incelenebileceği yeni araştırma yönleri oluşturulabileceğini göstermektedir.

Yazar bazında incelendiğinde, Zefferer Thomas en üretken yazar olarak öne çıkmaktadır. Şekil 1'de yer alan ortak yazar ağ haritasında da Zefferer'in farklı araştırmacılarla çok sayıda iş birliği yaptığı görülmektedir. Bu durum, e-imza güvenliği alanında belirli bir araştırma çekirdeği oluştuğunu ve disiplinler arası iş birliklerinin giderek arttığını göstermektedir.

Ülkeler düzeyinde yapılan analiz sonucunda, en fazla yayının ABD, Çin, Avusturya ve Almanya tarafından üretildiği görülmektedir. Bu ülkeleri Fransa, Ukrayna, İngiltere, Finlandiya, İspanya, Kanada ve Hollanda takip etmektedir. Bu tablo, e-imza güvenliği konusundaki araştırma faaliyetlerinin daha çok gelişmiş ekonomilerde ve dijital dönüşüm sürecini erken başlatan ülkelerde yoğunlaştığını göstermektedir. Ancak, gelişmekte olan ülkelerdeki sınırlı sayıdaki yayın, bu alanda daha fazla bölgesel çalışma yapılmasının gerekliliğine işaret etmektedir. Özellikle Türkiye gibi dijital dönüşüm sürecinde olan ülkelerde hem teknik hem de hukuki boyutlarıyla e-imza güvenliğini ele alan araştırmaların artırılması önerilmektedir.

Elde edilen bulgular, e-imza güvenliğinin yalnızca teknik değil, aynı zamanda hukuki ve yönetsel bir konu olduğunu da göstermektedir. Literatürde farklı ülkelerde yürürlükte olan e-imza yasaları arasında önemli farklar bulunduğu görülmüştür. Örneğin Zhang vd. (2021) tarafından yapılan çalışmada, Avrupa Birliği'ndeki eIDAS Yönetmeliği ile Amerika Birleşik Devletleri'ndeki ESIGN ve UETA yasalarının farklı yaklaşımlar benimsediği, bu nedenle uluslararası düzeyde uyumluluk sorunları ve hukuki belirsizliklerin ortaya çıktığı ifade edilmiştir. Bu durum, küresel ölçekte e-imza uygulamalarında ortak standartların ve yasal uyumun geliştirilmesi gerekliliğini ortaya koymaktadır.

Sonuç ve Öneriler

Bu çalışma e-imza güvenliği konusunda çalışan araştırmacılar için kaynak sunmakla birlikte, sonuçlar birtakım kısıtlar dahilinde ele alınmalıdır. Çalışmada incelenen kaynaklar yalnızca Scopus veri tabanı ile sınırlandırılmıştır. Bu durum, özellikle Türkçe literatürde yer alan çalışmaların büyük bir kısmının analize dâhil edilememesine neden olmuştur. Ayrıca analizde ele alınan çalışma sayısının sınırlı olması, konuya ilişkin eğilimlerin daha geniş bir perspektiften değerlendirilmesini güçleştirmektedir. Bu nedenle gelecekte yapılacak çalışmalarda farklı veri tabanlarının da (Web of Science, IEEE Xplore, Google Scholar vb.) kullanılması önerilmektedir.

Elde edilen bulgular, e-imza güvenliği araştırmalarının giderek teknolojik çeşitliliğe ve disiplinler arası iş birliklerine dayandığını göstermektedir. Kriptografik algoritmaların

geliştirilmesi, blokzincir temelli güvenlik modellerinin uygulanması ve kuantum bilişim çağında yeni imza protokollerinin tasarlanması bu alanın temel yönelimleri arasında yer aldığını göstermektedir. Ayrıca makine öğrenimi ve yapay zekâ temelli sahte imza tespit sistemleri gibi yeni nesil yaklaşımlar da e-imza güvenliği literatürüne katkı sağlayacak potansiyele sahiptir.

Elektronik imzaların güvenliği, bir dizi teknolojiyi, metodolojiyi ve yasal düzenlemeyi kapsayan çok boyutlu bir konudur. Kriptografik tekniklerin, biyometrik kimlik doğrulamanın, blokzincir teknolojisinin ve yasal çerçevelerin entegrasyonu, e-imzaların güvenilirliğini artırmak açısından kritik öneme sahiptir. Dijital işlemler modern toplumun giderek ayrılmaz bir parçası haline geldikçe, bu alanda sürdürülecek araştırmaların hem teknik hem de hukuki boyutlarıyla geliştirilmesi gerekmektedir.

Ayrıca e-imza güvenliği alanında yapılacak çalışmalarda uluslararası iş birliği ağlarının, bölgesel farklılıkların ve kullanıcı farkındalığının da analiz edilmesi önerilmektedir. Bu tür araştırmalar hem teknolojik altyapıların güçlendirilmesine hem de küresel düzeyde güvenli dijital kimlik yönetimi standartlarının oluşturulmasına katkı sağlar niteliktedir. Bu bağlamda, gelecekte yapılacak bibliyometrik çalışmalarda farklı veri tabanlarının kullanılması ve daha geniş anahtar kelime kümeleriyle analizlerin tekrarlanması, e-imza güvenliği literatürünün daha kapsamlı biçimde değerlendirilmesine katkı sağlayacaktır.

Etik Kurul İzni

Bu çalışma etik kurul izni gerektirmemektedir.

Yazarlık Katkısı

Yazarlar çalışmaya eşit katkı sağlamıştır.

Yazar Çatışması

Yazarlar herhangi bir çıkar çatışması olmadığını beyan etmektedir.

Benzerlik Taraması

Çalışmanın benzerlik oranı İntihal.net programından alınan rapora göre %7'dir.

Finansal Destek

Bu çalışma için herhangi bir finansal destek alınmamıştır.

Yapay Zekâ Kullanım Beyanı

Bu çalışmada yapay zekâ araçları yalnızca dil düzenleme ve yazım kontrolü amacıyla kullanılmıştır. Çalışmanın tüm bilimsel içeriği ve sorumluluğu yazarlara aittir.

Teşekkür

Yazarlar çalışmanın geliştirilmesine değerlendirme ve yönlendirmeleri ile katkıda bulunan hakemlere teşekkür ederler.

Kaynakça

Artsın, M. (2020). Bir Metin Madenciliği Uygulaması: VOSviewer. *Eskişehir Teknik Üniversitesi Bilim ve Teknoloji Dergisi B- Teorik Bilimler*, *8*(2), 344–354. https://dergipark.org.tr/en/pub/estubtdb/issue/56628/644637

Bengshir, T. K., & Topcan, F. (2008). Türkiye'de E-İmza Altyapısı Ve Kamu Kurumlarında Uygulamalar. *Amme İdaresi Dergisi*, *41*(1), 95–111.

Ber, A. S. (2022). Blokzincir (Blockchain) Teknolojisi Kapsamında Elektronik Çek. *Journal of Marine and Engineering Technology*, *2*(1), 1–20.

Borcoşi, C. A., Borcoşi, I., Marian, M., Cusman, A., & Ionică, D. (2023). Sustainability of Romanian Small and Medium Enterprises Using the Electronic Signature as A Driving Digital Tool. *Sustainability*, *15*(22), 15806. https://doi.org/10.3390/su152215806

Çoban, M. (2023). Türkiye'de E-Sağlık Uygulamalarında Mevcut Durum. *Bingöl Üniversitesi Sağlık Dergisi*, *4*(1), 197–204.

Djajadi, A., Lestari, K. S., Englista, L. E., & Destaryana, A. (2023). Blockchain-Based E-Certificate Verification and Validation Automation Architecture to Avoid Counterfeiting of Digital Assets in Order to Accelerate Digital Transformation. *CCIT Journal*, *16*(1), 68–85. https://doi.org/10.33050/ccit.v16i1.2367

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital Signature Scheme for Information Non-Repudiation in Blockchain: A State-of-The-Art Review. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1). https://doi.org/10.1186/s13638-020-01665-w

Güler, M., & Ömürgönülşen, U. (2011). Türkiye'de E-İmza Alanındaki Hukuki Düzenlemeler ve Bazı Kamu Kurumlarındaki E-İmza Uygulamaları. *Sosyoekonomi*, *14*(14), 202.

Haikal, M. N., & Mahmudah, S. (2024). *Implementation, Advantages and Barriers and Legal Protection Against the Use of Electronic Signatures*. Journal of Social Research, 3(6), 1179–1195. https://doi.org/10.55324/josr.v3i6.2067

Jadhav, G. G., Patil, P. D., & Kumbhar, V. S. (2025). Signature Verification System Using Machine Learning and Image Processing. Internati*onal Journal on Advanced Computer Engineering and Communication Technology*, *14*(1), 108–114.https://doi.org/10.65521/ijacect.v14i1.202

León, C. A. A. (2023). *La Prueba Documental De Fuentes İnformáticas Basadas En Documentos Digitales Con Firma Electrónica Certificada: Un Análisis Desde La Perspectiva De Las Tecnologías De La İnformación Y El Principio De Libertad De Prueba En El Proceso Penal Venezolano*. Revista Chilena de Derecho y Tecnología, 12(1), 10-12. https://doi.org/10.5354/0719-2584.2023.68567

Sağıroğlu, Ş., & Alkan, M. (2005). *Her Yönüyle Elektronik İmza (e-imza).* Grafiker Yayınları. Ankara.

Tarable, A., Paganelli, R. P., Storelli, E., Gatto, A., & Ferrari, M. (2025). *Generalized Quantum-Assisted Digital Signature*. IEEE Transactions on Quantum Engineering, 6, 1–11. https://doi.org/10.1109/tqe.2025.359570

Toubiana, R., Macdonald, M., Rajananda, S., Lokvenec, T., Kingsley, T. C., & Romero-Brufau, S. (2022). Blockchain for Electronic Vaccine Certificates: More Cons Than Pros? *Frontiers in Big Data*, *5*, 833196. https://doi.org/10.3389/fdata.2022.833196

Wang, W., Yu, Y., & Du, L. (2022). Quantum Blockchain Based on Asymmetric Quantum Encryption and A Stake Vote Consensus Algorithm. *Scientific Reports*, *12*(1). https://doi.org/10.1038/s41598-022-12412-0

Wang, Y. (2024). Online Electronic Signature Recognition Using Sparse Classification Techniques That Support Neural Models. *Journal of Computational Methods in Sciences and Engineering*, *24*(1), 263–275. https://doi.org/10.3233/JCM-237025

Zhang, L., Xie, J., & Liu, J. (2021). Electronic Signature Laws and Global E-Government Adoption: Comparative Analysis. *Government Information Quarterly*, *38*(2), 101552. https://doi.org/10.1016/j.giq.2021.101552

Zefferer, T. (2014, December). A Server-Based Signature Solution for Mobile Devices. In *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia* (pp. 175–184). https://doi.org/10.1145/2684103.2684142

EXTENDED SUMMARY

Research Problem

Electronic signature systems are important technological structures used to ensure the accuracy and security of digital signatures. Although e-signature security is a multidimensional field with technological, legal, and practical aspects, it is observed that bibliometric analyses systematically revealing the general trends and research orientations in this field are limited. This study aims to conduct a bibliometric analysis of research on e-signature security.

Research Questions

- Within the scope of this study, answers were sought to the following questions:
- What is the general distribution of studies conducted in the field of e-signature security?
- Who are the authors with the highest number of publications in this field?
- Which studies and authors receive the highest number of citations?
- Around which concepts do the keywords concentrate?
- What is the distribution of authors in terms of their institutions and countries?

Literature Review

In the literature on e-signature security, the applicability of different security protocols and security approaches has been emphasized. Electronic signatures are widely preferred in security-sensitive applications such as e-government services and e-banking. These digital signatures are used to ensure the accuracy and security of transactions.

The literature review revealed that although there are various studies in terms of content in the field of e-signature security, no bibliometric analysis study has been conducted. This situation indicates that the general trends, research orientations, and collaboration networks of the field have not been systematically examined.

Methodology

This study is quantitative research and employs the bibliometric analysis method. Bibliometric analysis is based on examining and analyzing the document obtained according to specific characteristics.

During the analysis process, the keywords “security” and “electronic signature” were searched in the Scopus database covering the years 1979–2024, and 487 documents were reached. The retrieved documents were analyzed using the VOSviewer program.

The bibliometric analysis includes:

- Co-authorship analysis
- Author citation analysis
- Keyword analysis
- Authors' institutions
- Authors' countries

Findings and Results

As a result of the study, it was determined that there is not a sufficient number of publications in the field of e-signature security. It is observed that even the authors with the highest number of publications have a limited number of studies.

It was determined that the first three authors with the highest number of citations have the same citation count. The keyword analysis results show that the literature largely concentrates around the concepts of "e-signature," "security," "electronic signature," and "authentication."

Overall, the findings reveal that certain themes are dominant in the field of e-signature security, whereas new technological approaches have not been examined in sufficient depth.

It has been concluded that up-to-date studies should be increased to ensure e-signature security. In addition, conducting studies using different databases and broader keyword sets is considered to contribute to a more comprehensive evaluation of the field.