ISSN: 3023 - 8544

ADBA COMPUTER SCIENCE

VOLUME 2, ISSUE 1, JANUARY 2025

AN INTERDISCIPLINARY JOURNAL OF COMPUTER SCIENCE

https://journals.**adbascientific**.com/acs

ISSN: 3023 - 8544

ADBA Computer Science
Cutting-Edge Scientific Solutions

Volume: 2 – Issue No: 1 (January 2025)
https://journals.adbascientific.com/acs/issue/view/6

Editorial Board Members

ISSN: 3023 - 8544

ADBA Computer Science
Cutting-Edge Scientific Solutions

Volume: 2 – Issue No: 1 (January 2025)
https://journals.adbascientific.com/acs/issue/view/6

Contents:

ADBA Computer Science
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8544
RESEARCH ARTICLE
Vol.2 / No.1 / 2025 / pp.1-6
https://doi.org/10.69882/adba.cs.2025011

The Role of Technological Approaches in Cyber Security of Autonomous Vehicles

Ebubekir Seyyarer [*,1], **Faruk Ayata** [α,2] **and Selim Özdem** [β,3]

*Van Yüzüncü Yıl University, Computer Engineering, Van, 65090, Türkiye, [α]Van Yüzüncü Yıl University, Başkale Vocational High School, Van, 65090, Türkiye, [β]Hitit University, Alaca Avni Çelik Vocational High School, Çorum, 19030, Türkiye.

ABSTRACT Autonomous vehicles play a significant role in future transportation systems by enabling driverless travel. These vehicles offer advantages such as reducing accidents, improving travel times, and conserving energy. However, ensuring the independent operation of these technologies requires robust cybersecurity measures. Protecting autonomous vehicles against security threats they may face within their internal systems or during communication with other vehicles and infrastructure is crucial. This study examines the security measures used in autonomous vehicles. Encryption and data protection techniques safeguard information from unauthorized access during in-vehicle and inter-vehicle communication. Additionally, intrusion detection and prevention systems (IDS/IPS) detect abnormal activities to protect against potential threats. Machine learning-based anomaly detection methods analyze data from sensors and network traffic to identify emerging threats. Regular software updates help mitigate vulnerabilities, while network segmentation isolates different systems to protect critical components. Multi-layered security solutions ensure the safe operation of autonomous vehicles. These approaches contribute to the development of future security standards.

KEYWORDS
Autonomous vehicles
Cybersecurity threats
Autonomous vehicle security
Artificial intelligence

INTRODUCTION

Autonomous vehicle technologies have an important place among the transportation solutions of the future thanks to their ability to drive without driver intervention. Autonomous vehicles offer benefits such as reducing traffic accidents, optimizing travel times and increasing energy efficiency, and therefore have great potential for both individual users and social infrastructure. However, the ability of these vehicles to drive autonomously and safely requires the implementation of advanced safety measures. In particular, autonomous vehicles must be protected from cybersecurity threats that they may encounter both in their on-board systems and when communicating with other vehicles and infrastructure.

Cybersecurity methods developed to ensure the safety of autonomous vehicles provide a multi-layered structure that aims to protect vehicles against different types of attacks. This study discusses a wide range of solutions, from encryption techniques to enhance in-vehicle data security and communication security, to intrusion detection and prevention systems (IDS/IPS) used to detect anomalous behavior, to machine learning-based anomaly detection methods and physical security measures such as vehicle network segmentation. While encryption and data security prevent malicious individuals from intercepting data in the vehicle and in communication between vehicles, IDS and IPS systems provide protection against potential threats by detecting abnormal activity in the system.

In addition, anomaly detection based on machine learning analyzes the data obtained from vehicle sensors and network traffic, enabling the detection of unknown threats. In this way, an effective defense can be ensured even against previously unidentified types of attack. In addition, secure software and system updates enable the secure implementation of software updates for vehicles so that security gaps can be closed quickly. The segmentation of the in-vehicle network aims to isolate critical systems by dividing the network into different sections and preventing security risks from spreading to other systems.

Özarpa *et al.* (2021) examines the vulnerabilities in the wireless connectivity and operating systems of autonomous vehicles and states that these vulnerabilities should be detected using tools such as NMAP, Maltego and Metasploit. The study highlights that

Manuscript received: 10 December 2024,
Revised: 22 January 2025,
Accepted: 24 January 2025.

[1]eseyyarer@yyu.edu.tr (**Corresponding author**).
[2]fayata@yyu.edu.tr
[3]selimozdem@hitit.edu.tr

vehicles are vulnerable to external attacks and states that these vulnerabilities should be addressed with continuous monitoring and up-to-date security protocols. It is concluded that vehicle systems should be monitored regularly.

Çakal *et al.* (2021) addresses communication security issues between autonomous vehicles and explains the importance of lightweight security protocols, especially in vehicles with IoT sensors. The study evaluates cryptography algorithms and attack mitigation techniques, analyzes vulnerabilities in networks such as VANETs and recommends the use of lightweight encryption techniques. It concludes that lightweight cryptography algorithms support low-latency operation.

Durlik *et al.* (2024) examines threats such as remote hacking, sensor tampering and denial of service (DoS) in autonomous vehicles and evaluates the defense methods against these threats. The study examines encryption, IDS systems, regular updates and authentication methods and points to the potential of advanced technologies such as artificial intelligence and blockchain for cybersecurity. It notes that security problems persist due to the complexity of vehicles.

Abouabdalla and Goyal (2022) analyzes the most vulnerable areas in autonomous vehicles and offers solutions for points of attack such as GPS, sensors and network connections. The study proposes machine learning and data encryption techniques, but notes that the success of these methods has not been directly tested. Hypothetical solutions for the security of autonomous vehicles are developed.

Saeed *et al.* (2023) examines the current cybersecurity threats to connected and autonomous vehicles (CAV) and provides applicable solutions to these threats. The study analyzes attacks on LiDAR, GPS and other sensors and highlights the importance of authentication, data encryption and IDS methods. It also states that cooperation between manufacturers should be strengthened.

The multi-layered cybersecurity approaches examined in this study have the potential to contribute to the reduction of security vulnerabilities in autonomous vehicles and the creation of a sustainable security infrastructure. This study offers the following contributions:

- Standardization of Cybersecurity Protocols: Multi-layered security measures such as encryption, attack detection and prevention systems, and machine learning-based anomaly detection methods developed for autonomous vehicles should be brought together within the framework of international standards. This will increase compatibility between vehicle manufacturers and software developers and ensure that security vulnerabilities are prevented more effectively.
- Optimisation of Artificial Intelligence-Based Threat Detection Systems: Machine learning and artificial intelligence techniques should be optimised to dynamically detect security vulnerabilities in autonomous vehicles. These systems should be developed to predict not only current threats but also complex cyber attacks that may arise in the future.
- The present study proposes a more comprehensive testing and integration process for the verification of security measures employed in autonomous vehicles. The integration of security systems with diverse in-vehicle network structures and infrastructures is intended to establish an ecosystem that exhibits enhanced resistance to cyber threats.

The remainder of the study is structured as follows: the second section provides an exposition on in-vehicle and inter-vehicle data encryption security. The third section provides information about attack detection and prevention systems in autonomous vehicles.The fourth section provides an explanation of anomaly detection in the security systems of autonomous vehicles using machine learning methods.The fifth, sixth and seventh sections explain the installation of secure software in autonomous systems, the updating of the system, in-vehicle segmentation and physical security measures that can be taken. The final section of the study presents the results of the research and puts forward recommendations for future research and development in this field.

MATERIALS AND METHODS

Data Encryption Security

Encryption of data in vehicle and vehicle-to-vehicle communication is one of the cornerstones of modern cyber security procedures. This method plays a crucial role in ensuring the security of both individual vehicles and vehicle networks. Encryption techniques prevent malicious individuals from intercepting or manipulating this data by ensuring that the transmitted data can only be read by authorized recipients. Particularly in autonomous and connected vehicle technologies, encryption applications provide an important layer of security for GPS location data, sensor data, driving commands and vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications (Stallings 2016; Schneier 2007).

Strong encryption algorithms use a combination of symmetric and asymmetric encryption techniques to secure data (Figure 1 and Figure 2). Symmetric encryption uses the same key to encrypt and decrypt data, while asymmetric encryption uses a different key for encryption and decryption. These methods offer advantages in terms of speed and security. For example, symmetric algorithms such as AES (Advanced Encryption Standard) are efficient in terms of speed; asymmetric algorithms such as RSA (Rivest-Shamir-Adleman) provide a higher level of security.

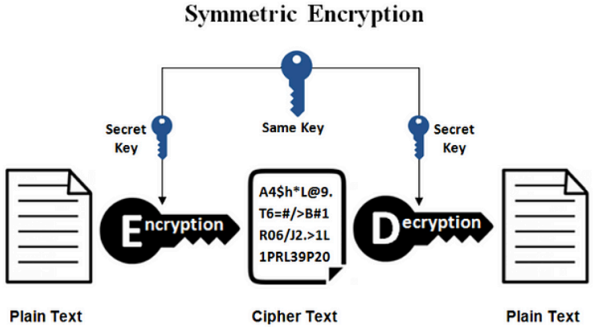


Figure 1 Symmetric encryption (Özkan 2020).

Intrusion Detection and Prevention Systems

In order to ensure network and system security in autonomous vehicles, intrusion detection and prevention systems are used. These systems identify abnormalities by learning normal behaviors and apply the necessary precautions (Scarfone and Mell 2007; Modi *et al.* 2013).

Intrusion Detection System (IDS): Intrusion Detection System (IDS) is a security solution used to detect threats by monitoring network traffic and system activities. IDS plays a critical role in detecting security breaches or attacks that may occur in a system. However, IDS provides a passive defense; it only detects and reports threats, but does not have the authority to directly

Table 1 Comparison of symmetric and asymmetric encryption (Avaroğlu 2022)

Subject	Symmetric	Asymmetric
Confidentiality	Provides	Provides
Integrity	-	Provides
Authentication	-	Provides
Non-repudiation	-	Provides
Performance	Fast	Slow
Security	Depends on key length	Depends on key length

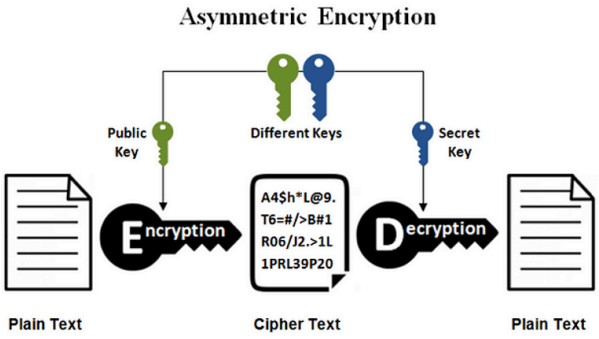


Figure 2 Asymmetric encryption (Özkan 2020)

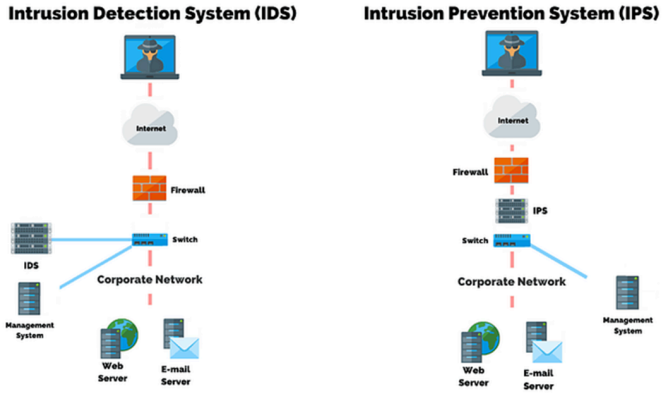


Figure 3 IDS and IPS working architecture (Aydogan 2022).

block or stop these threats. Therefore, IDS usually requires manual intervention by security teams (Northcutt and Novak 2002).

IDS has two basic modes of operation: Network-Based IDS (NIDS) and Host-Based IDS (HIDS). NIDS analyzes network traffic to detect anomalous behavior or known attack patterns. For example, it scans data packets on the network to identify intrusion or malicious traffic Roesch (1999). HIDS, on the other hand, works on a specific device or host. This type of IDS detects possible changes or anomalies in the system by monitoring file integrity and transaction logs (Scarfone and Mell 2007).

IDS uses two different methods to detect attacks: Signature-Based Detection and Anomaly-Based Detection. Signature-based detection identifies attacks using known threat signatures. The system compares data packets with predetermined signatures and sends an alert when there is a match (Modi *et al.* 2013).

On the other hand, anomaly-based detection learns the normal behavior of the system and detects threats when there is a deviation from these behaviors. This method is especially effective in detecting previously unidentified types of attacks (Chandola *et al.* 2009).

When IDS detects threats, it sends reports to security teams or system administrators. However, due to the passive nature of these systems, they cannot directly intervene in threats. This shows that IDS should be supported by active defense systems such as IPS (Scarfone and Mell 2007).

Intrusion Prevention System (IPS): IPS monitors network traffic and system activities similar to IDS, but takes a more active approach. IPS not only reports threats after detecting them, but also automatically intervenes in them. This feature makes IPS an effective system in quickly stopping security threats. For example, when suspicious activity is detected on the network, IPS can stop this traffic and prevent malicious interactions (Bace *et al.* 2001).

IPS usually works at a central point where network traffic passes and analyzes this traffic to identify potential threats. The system is integrated with firewalls to examine incoming packets and block suspicious movements. Thanks to detailed analysis of traffic, IPS increases system security and prevents malicious packets from entering the network (Modi *et al.* 2013). This structure makes it possible to detect threats at an earlier stage and neutralize them. IPS can respond quickly to threats with detection methods. Signature-based detection methods are used to identify known threats, while anomaly-based methods learn the normal behavior of the system and perceive deviations as threats. In order to intervene in detected threats, IPS applies methods such as stopping malicious packets, blocking specific IP addresses, or redirecting traffic. In this way, harmful effects on the system are minimized (Sommer and Paxson 2010).

The effectiveness of IPS is more clearly seen in practical examples. For example, in a Distributed Denial of Service (DDoS) attack, IPS can analyze excessive traffic and eliminate this load and ensure uninterrupted operation of services (Mirkovic and Reiher 2004). In addition, malicious files or suspicious traffic detected in the network can be quarantined by IPS, preventing damage to the system (Amini and Qian 2017).

IDS and IPS Working Together: Most modern security systems combine IDS (Intrusion Detection System) and IPS (Intrusion Pre-

vention System) functions to provide more effective protection. While IDS detects and reports threats on the network or system, IPS intervenes immediately to prevent attacks. This combination creates a fast and proactive defense mechanism against security threats (Modi et al., 2013). Thanks to this compatible structure, IDS and IPS work together, allowing security teams to identify threats faster. Suspicious activities detected by IDS can be automatically stopped by IPS. In this way, threats are effectively prevented. This collaboration offers a great advantage in providing real-time protection, especially in institutions with complex network structures or critical infrastructures.

Machine Learning Based Anomaly Detection

Autonomous vehicles provide independent movement capability by working with advanced sensors, complex algorithms and continuous data exchange. While this technological structure provides great advantages in terms of security, it can also become vulnerable to various security threats. Machine learning-based methods stand out as an effective defense mechanism against these threats (Ayata and Seyyarer 2022). These methods undertake important functions such as detection of abnormal behavior, attack prediction and prevention of potential threats (Hodge and Austin 2004; Chandola *et al.* 2009). Table 2 provides the pros and cons of these methods.

Anomaly Detection: Autonomous vehicles use machine learning algorithms to detect anomalous behavior in their systems. For example, data from sensors are continuously analyzed to establish normal behavior patterns of the system. Anomaly detection algorithms detect deviations from this normal flow and warn of potential threats. For example, sudden speed changes or unexpected GPS data can be a sign that the system may be targeted. These algorithms increase vehicle safety by detecting potential threats at an early stage (Ahmed *et al.* 2016).

Intrusion Detection and Prevention: Machine learning plays an important role, especially in detecting and preventing cyberattacks. Unsupervised learning methods are used to detect unknown types of attacks in network traffic (Seyyarer and Ayata 2023). These algorithms learn the normal flow of network traffic and evaluate deviations from this flow as attacks. For example, during vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication, machine learning-based systems can automatically flag suspicious data packets (Chandola *et al.* 2009; Sommer and Paxson 2010).

Real-Time Threat Management: Real-time data analysis is crucial for the safety of autonomous vehicles. Deep learning models, in particular, can detect threats in real time by analyzing complex data sets. For example, recurrent neural networks (RNN) or autoencoders process data from vehicle sensors to identify potential security threats. These models can predict future threats by examining past data. This ability allows vehicles to be better prepared for environmental risks (Goodfellow 2016).

Secure Software And System Updates

Safe software updates in autonomous vehicles are a critical requirement to ensure system security. Over-the-air (OTA) updates allow regular and protected updates of software and security patches in vehicles (Macher *et al.* 2017; Medvedev and Vybornova 2018). This method provides a flexible and secure solution for the smooth operation of autonomous vehicles.

Update Process:

- Preparation of Update Package: Developer teams create software updates and add security patches. The update package is usually compressed and uploaded to the server. For security, the authenticity and identity of the package is verified using a digital signature (Nguyen *et al.* 2020).
- Secure Data Transmission: The update is securely transferred from the server to the devices. Data transfer is provided using encryption methods such as HTTPS or TLS. The device checks whether an appropriate update is available by sending software version information to the server (Hossain *et al.* 2015).
- Installing the Update on the Device: The update package is downloaded to the device's memory and stored in a temporary area. The integrity of the file is checked with digital signature verification. The device can continue to operate during the update, so there is no operational interruption. When the installation is complete, the device is restarted and the new software is put into operation (Macher *et al.* 2017).
- Rollback Mechanism: If the update fails or an error is detected, the rollback function is activated. In this way, the device can return to the previous software version and be ready for the update again (Nguyen *et al.* 2020).
- Post-Update Reporting: After successful updates, the device sends an update report to the server. This report is used to analyze statistics and investigate possible problems (Medvedev and Vybornova 2018).

Safe OTA Update Principles:

- Digital Signature: Digital signing is used to protect update packages against counterfeit software (Nguyen et al., 2020)
- Rollback Function: Allows the device to revert to the previous version if a problem occurs after the update (Medvedev and Vybornova 2018).
- Network Security: Encryption protocols such as HTTPS or TLS should be used to increase security during data transfer (Hossain *et al.* 2015).
- Verification Mechanisms: Version and device information must be verified to ensure that the update package is compatible with the device (Nguyen *et al.* 2020).

In-Vehicle Segmentation

Segmentation of the network within the vehicle is a critical method used to increase system security. Network segmentation prevents the attack from spreading to other components if one component is attacked. In particular, isolating critical systems such as braking and steering from less critical systems such as entertainment or navigation increases the overall security of the vehicle (Wolf and Serpanos 2017; Bosch *et al.* 1991) .

Network Segmentation: The network inside the vehicle is divided into separate sections for different systems and functions. Each network section is isolated from other sections, limited to a specific system. For example, critical safety systems such as brakes and steering operate independently of less important systems such as entertainment and navigation. This structure prevents security breaches in one area from spreading to other areas. Thus, a higher level of security is provided throughout the system (Groll and Rumez 2019).

Use of Different Network Protocols: The different systems in the vehicle are usually separated by various protocols such as CAN (Controller Area Network), LIN (Local Interconnect Network), FlexRay and Ethernet. Critical systems use CAN and FlexRay

Table 2 Pros and Cons of machine learning based methods

Method	Pros	Cons
Anomaly Detection	Increases security by detecting potential threats at an early stage; provides rapid data analysis.	False positive rates can be high; requires accurate and high quality dataset for training.
Intrusion Detection and Prevention	It can detect unknown attacks and offers adaptive protection with its ability to continuously learn.	Requires high processing power; may affect the normal operation of the system.
Real-Time Threat Management	It analyzes complex data sets, can predict future threats and respond quickly.	Deep learning models are costly; real-time operation may experience delays.

protocols because they require fast and reliable communication. In contrast, entertainment and information systems that require high data rates usually operate on Ethernet. Communication between these protocols is provided through special gateways or firewalls (Koscher *et al.* 2010).

Gateway Usage: Devices called "gates" are used to regulate data exchange between segments. Gates control data transfer between two different networks and block risky data packets. For example, gates that prevent direct data transmission from the entertainment system to the brake system protect sensitive systems. These devices limit unauthorized access to critical data while allowing certain data packets to pass through (Checkoway *et al.* 2011).

Firewalls and Filtering: Firewalls are activated to protect critical systems. These systems allow only authorized data packets to pass through and filter requests from external networks. Access requests, especially from internet-connected devices, are controlled by in-vehicle firewalls. Data exchange is only allowed within the framework of specified protocols, thus neutralizing attack attempts (Macher *et al.* 2017).

Access Control and Monitoring: Specific access controls are applied for each segment. For example, only certain devices can access the entertainment system, while the braking system is only open to approved electronic control units (ECUs). In addition, network traffic within the vehicle is constantly monitored. If unusual data transfers or abnormal behaviors are detected, the system issues warnings or activates automatic defense mechanisms (Wolf and Serpanos 2017).

Physical Security Measures

The physical security of autonomous vehicles is of critical importance in preventing unauthorized access and physical interventions. Secure hardware components, secure boot mechanisms, and physical tamper detection systems are the basic security solutions used to prevent threats to vehicle hardware (Wolf and Serpanos 2017).

Secure Boot: Secure Boot verifies the reliability of the device's software components, allowing only authorized software to run. This mechanism ensures that malware or unauthorized changes are disabled during system startup. Working Principle: Secure Boot creates a hardware-supported trust chain (Root of Trust). During system startup, each software component is verified with a digital signature by the previous component. For example, components such as the bootloader and the operating system kernel are only run when the verification is successful. If the digital signature cannot be verified, the system startup process is stopped, thus preventing unsafe software from running (Wolf and Serpanos 2017).

Physical Intervention Detection Systems: Physical tamper detection systems detect unauthorized access or interventions by protecting the physical security of the device. These systems detect physical tampering attempts and take appropriate security measures to ensure the protection of sensitive components.

Working Principle: These systems detect physical interventions through sensors and detectors located on the device. Components such as magnetic sensors, optical sensors, pressure sensors and light sensors are placed on the external structure of the device or on hardware components. When an unusual physical change is detected on the device, the system automatically gives an alarm, applies a process interruption or puts sensitive data into protection mode (Van Eck *et al.* 2017).

Interoperability; Secure Boot and Physical Tamper Detection: Secure Boot and tamper detection systems are used together to ensure both software and physical security of a device. Secure Boot ensures that only verified and trusted software is run, while physical tamper detection systems ensure that the device is protected from external tampering. This combination is particularly popular in security-critical areas such as autonomous vehicles, financial sector devices (e.g. ATMs), and healthcare systems. For example, in an autonomous vehicle, Secure Boot ensures that the vehicle is operating in a secure software environment, while physical tamper detection prevents unauthorized access to components on the vehicle (Van Eck *et al.* 2017).

CONCLUSION

The integration of autonomous vehicle technologies within future transportation systems is of paramount importance, given the safety, efficiency and environmental benefits they offer. However, in order to ensure the safe and smooth operation of these vehicles, it is imperative to implement robust cybersecurity measures. A comprehensive approach to cybersecurity is necessary to safeguard both in-vehicle systems and inter-vehicle communication networks. Multi-layered cybersecurity methods contribute to the creation of a sustainable infrastructure by reducing the security vulnerabilities of autonomous vehicles.Encryption techniques, intrusion detection and prevention systems (IDS/IPS), machine learning-based anomaly detection, secure software updates and in-vehicle network segmentation are among the main methods used

to increase autonomous vehicle security.These technologies not only detect threats, but also prevent potential attacks and prevent damage to the functioning of the systems. Of particular note are the innovative solutions offered by artificial intelligence and machine learning-based technologies, which demonstrate superior performance against dynamic and complex threats. As autonomous vehicles become more prevalent, there is an increasing necessity for the continuous development of security standards and their integration into vehicle designs. This study provides a framework for meeting security requirements, thereby facilitating the safe and effective introduction of these innovative technologies into society. Cybersecurity is an indispensable element for the adoption of autonomous vehicles and their potential social benefits.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Abouabdalla, K. O. and S. B. Goyal, 2022 Autonomous vehicles: Improving cyber security. International Journal of Advanced Research in Technology and Innovation **4**: 118–126.

Ahmed, M., A. Naser Mahmood, and J. Hu, 2016 A survey of network anomaly detection techniques. J. Netw. Comput. Appl. **60**: 19–31.

Amini, S. and C. Qian, 2017 A survey on network security monitoring in high-speed networks. IEEE Communications Surveys & Tutorials **20**: 3271–3290.

Avaroğlu, E., 2022 Bilgi güvenliğinin temel yapi taşi: Kriptoloji. Düşünce Dünyasında Türkiz **8**: 53–65.

Ayata, F. and E. Seyyarer, 2022 *The Most Important Defense System of the Technology Age: Cyber Security. Yenilenebilir Kaynaklardan Elde Edilen Malzemeler ve Uygulamaları*. Artikel Akademi, İstanbul.

Aydogan, M., 2022 Saldırı tespit sistemleri (ids) & İzinsiz giriş Önleme sistemleri (ips). Erişim tarihi: 25 Ocak 2025.

Bace, R. G., P. Mell, *et al.*, 2001 Intrusion detection systems .

Bosch, R. *et al.*, 1991 Can specification version 2.0. Rober Bousch GmbH, Postfach **300240**: 72.

Çakal, K., İ. Kara, and M. Aydos, 2021 Cyber security of connected autonomous vehicles. Avrupa Bilim ve Teknoloji Dergisi pp. 1121–1128.

Chandola, V., A. Banerjee, and V. Kumar, 2009 Anomaly detection. ACM Comput. Surv. **41**: 1–58.

Checkoway, S., D. Mccoy, B. Kantor, D. Anderson, H. Shacham, *et al.*, 2011 Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the USENIX Security Symposium*, pp. 77–92.

Durlik, I., T. Miller, E. Kostecka, Z. Zwierzewicz, and A. Łobodzińska, 2024 *Cybersecurity in Autonomous Vehicles-Are We Ready for the Challenge?*, volume 13. Electronics.

Goodfellow, I., 2016 Deep learning.

Groll, A. and M. Rumez, 2019 Security aspects of automotive over-the-air updates. In *IEEE International Conference on Vehicular Electronics and Safety*, pp. 1–6.

Hodge, V. J. and J. Austin, 2004 A survey of outlier detection methodologies. Artificial Intelligence Review **22**: 85–126.

Hossain, M. M., M. Fotouhi, and R. Hasan, 2015 Towards an analysis of security issues, challenges, and open problems in the internet of things. IEEE World Congress on Services pp. 21–28.

Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, *et al.*, 2010 Experimental security analysis of a modern automobile. In *IEEE Symposium on Security and Privacy*, pp. 447–462.

Macher, G., H. Sporer, E. Armengaud, and C. Kreiner, 2017 OTA updates in automotive systems: Why and how to ensure safety and security. Journal of Automotive Software Engineering **3**: 45–58.

Medvedev, K. and E. Vybornova, 2018 Over-the-air update protocol for internet of things. In *IEEE Conference Proceedings*.

Mirkovic, J. and P. Reiher, 2004 A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review **34**: 39–53.

Modi, C., D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, 2013 A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications **36**: 42–57.

Nguyen, T. K., T. T. Hoang, and T. Q. Ha, 2020 Securing over-the-air software updates for IoT and autonomous vehicles. International Journal of Security and Networks **15**: 1–12.

Northcutt, S. and J. Novak, 2002 *Network intrusion detection*. Sams Publishing.

Özarpa, C., İ. Avcı, and S. A. Kara, 2021 Otonom araçlar için siber güvenlik risklerinin araştırılması ve savunma metotları. Avrupa Bilim ve Teknoloji Dergisi pp. 242–255.

Roesch, M., 1999 Snort - lightweight intrusion detection for networks. In *Proceedings of the 13th USENIX Conference on System Administration*, pp. 229–238.

Saeed, Z., M. Masood, and M. U. Khan, 2023 A review: Cybersecurity challenges and their solutions in connected and autonomous vehicles (CAVs). JAREE (Journal on Advanced Research in Electrical Engineering) **7**.

Scarfone, K. and P. Mell, 2007 *Guide to intrusion detection and prevention systems (IDPS)*. NIST Special Publication.

Schneier, B., 2007 *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons.

Seyyarer, E. and F. Ayata, 2023 Siber güvenlikte makine öğrenimi dönemi .

Sommer, R. and V. Paxson, 2010 Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy*, IEEE.

Stallings, W., 2016 *Cryptography and network security: Principles and practice*. Pearson.

Van Eck, W., B. Kuijper, and L. Wagemans, 2017 Physical tamper detection in electronic devices: Technologies and application. Journal of Electronic Protection and Security **12**: 132–145.

Wolf, M. and D. Serpanos, 2017 *Embedded systems security: Foundations and applications*. Morgan Kaufmann.

Özkan, H., 2020 Simetrik ve asimetrik anahtarlı Şifreleme algoritmaları. Erişim tarihi: 25 Ocak 2025.

How to cite this article: Seyyarer, E., Ayata, F. and Özdem, S. The Role of Technological Approaches in Cyber Security of Autonomous Vehicles. *ADBA Computer Science*, 2(1), 1-6, 2025.

ADBA Computer Science
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8544
RESEARCH ARTICLE
Vol.2 / No.1 / 2025 / pp.7-14
https://doi.org/10.69882/adba.cs.2025012

High-Accuracy Prediction of Mechanical Properties of Ni-Cr-Fe Alloys Using Machine Learning

Yusuf Uzunoğlu [*,1], **Berkay Emin** [α,2] **and Yusuf Alaca** [β,3]

* Materials Science and Engineering, Erciyes University, 38039 Kayseri, Türkiye , [α]Electronics and Automation, Osmancik Omer Derindere Vocational College, Hitit University, Çorum, Türkiye, [β]Computer Engineering, Hitit University, 19030 Çorum, Türkiye.

ABSTRACT Artificial intelligence-driven prediction models have emerged as powerful tools for estimating material properties with high accuracy, yet the preparation of training datasets often demands labor-intensive and time-consuming experimental procedures. Leveraging the Computational Materials Science (CMS) approach, this study utilizes phase transformation calculations and thermodynamic data to simulate the mechanical properties of Ni-Cr-Fe alloys. Using JMatPro software, mechanical properties (0.2% Proof Stress, Fracture Stress, and Young's Modulus) of 50 Ni-Cr-Fe alloy compositions were simulated across a temperature range of 540–920 ℃, generating a dataset of 1000 rows. This dataset was used to train an Artificial Neural Network (ANN) model, with 80% allocated for training and 20% for validation and testing. The trained AI model demonstrated robust predictive capabilities, achieving a 96.61% accuracy rate in forecasting material compositions with the desired thermo-physical properties at specific temperatures. To validate the model's reliability, predicted alloy compositions were re-simulated under identical conditions in JMatPro, confirming the high fidelity of the model's predictions. The results underscore the efficacy of Computational Materials Science (CMS)-generated datasets as a scalable and reliable source for training AI models in materials science. This study highlights the potential of integrating Computational Materials Science (CMS) and Machine Learning approaches to accelerate material design and development processes, delivering significant improvements in prediction speed and accuracy.

KEYWORDS
Computational materials science
Machine learning
Artificial neural networks
Alloy design
Nickel alloys

INTRODUCTION

The development of predictive tools for estimating material properties has become increasingly important in the design and optimization of advanced alloys. Machine Learning (ML), as a data-driven approach, has shown remarkable potential in this domain by enabling the rapid prediction of mechanical, thermal, and thermodynamic properties. Recent studies highlight the effectiveness of Machine Learning models in understanding the complex interactions in multi-component systems such as Ni-Cr-Fe alloys, which are critical for high-performance applications due to their exceptional mechanical strength and corrosion resistance at elevated temperatures (Jain *et al.* 2023; Wang *et al.* 2021). These alloys are extensively used in aerospace, power generation, and chemical industries, where the optimization of their mechanical properties, such as yield strength, fracture toughness, and elasticity, is crucial (Mukhamedov *et al.* 2021).

Traditionally, experimental characterization of material properties has been labor-intensive, requiring extensive resources and time. The emergence of Computational Materials Science (CMS) has revolutionized this field by providing simulation-based insights into phase stability, stress-strain behavior, and thermodynamic properties. Tools like JMatPro have been instrumental in simulating the behavior of alloys under varied conditions, generating reliable datasets for machine learning applications (Filipoiu and Nemnes 2020; Liu *et al.* 2024). Leveraging these simulated datasets, Machine Learning models such as Artificial Neural Networks (ANNs) have demonstrated superior predictive accuracy, as seen in studies that model phase stability and hardness of high entropy alloys and other multi-component systems (Jeon *et al.* 2022; Chen *et al.* 2014).

In the context of Ni-Cr-Fe alloys, Machine Learning models have been utilized to explore the effects of compositional variations and temperature on mechanical properties. Studies employing physics-informed ML algorithms have successfully predicted thermodynamic and kinetic behaviors of chromium atoms in Fe-Ni-Cr systems, enhancing the understanding of stress-strain responses (Wang *et al.* 2021). Additionally, Machine Learning (ML)-driven methods have enabled the optimization of alloy compositions to achieve desired ductility, hardness, and elastic modulus (Jeon *et al.* 2022). Such approaches not only reduce dependency on experimental trials but also provide a pathway for exploring large compositional spaces effectively.

Manuscript received: 16 December 2024,
Revised: 25 January 2025,
Accepted: 27 January 2025.

[1]4012640009@erciyes.edu.tr (**Corresponding author**).
[2]berkayemin@hitit.edu.tr
[3]yusufalaca@hitit.edu.tr

This study aims to build upon these advancements by integrating Computational Materials Science (CMS) simulations and Machine Learning to predict the mechanical properties of Ni-Cr-Fe alloys. Using a dataset of 1000 rows simulated with JMatPro, an ANN model is trained to predict 0.2% proof stress, fracture stress, and Young's modulus across a temperature range of 540–920°C. The results indicate an accuracy exceeding 96.61%, demonstrating the robustness of this methodology. This work underscores the potential of combining simulation and Machine Learning to enhance alloy design, providing significant improvements in speed and precision compared to traditional methods.

MATERIALS AND METHODS

This study employs a Computational Materials Science (CMS)-based approach, leveraging the JMatPro software to simulate the mechanical properties of Ni-Cr-Fe-based nickel alloys. JMatPro, recognized for its ability to compute phase diagrams and thermodynamic properties, was utilized to generate a dataset comprising 1000 rows. These entries encompassed the mechanical properties of 50 distinct compositions, including elements such as Ni, Cr, Fe, Co, Mo, Nb, Ti, Al, Mn, Si, and Cu. The primary mechanical properties under investigation were 0.2% Proof Stress, Fracture Stress, and Young's Modulus, simulated across a temperature range of 540–920°C. The dataset was split into training (80%) and validation/testing (20%) subsets for model development and evaluation.

A Machine Learning (ML) model, specifically an Artificial Neural Network (ANN), was constructed to predict the mechanical properties of these alloys based on the CMS-generated dataset. As depicted in Figure 1, the model operates on a normalized dataset, where all input values were scaled between 0 and 1 using the Min-Max Normalization method. This preprocessing step ensures that the data are uniformly represented, facilitating effective learning by the ANN. To enhance dataset quality, missing values were addressed through multiple linear regression, ensuring the integrity and completeness of the input data. Additionally, all physical properties were converted into international SI units for consistency and further normalized before feeding into the model.

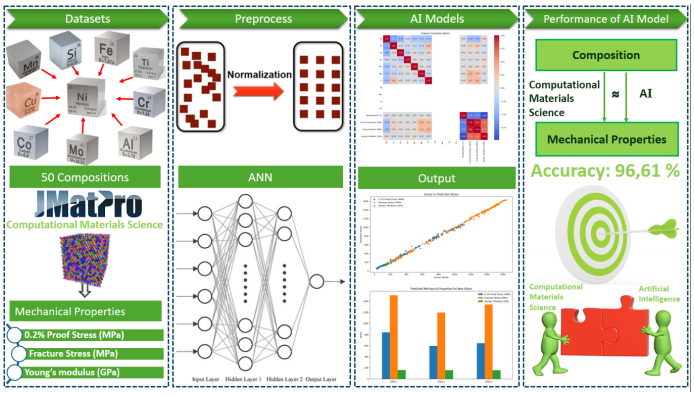


Figure 1 Flowchart of the proposed model for predicting the mechanical properties of Ni-Cr-Fe based nickel alloys

The proposed model (Figure 1) integrates the normalized data into a tensor structure, enabling efficient processing by the ANN architecture. The ANN was designed to capture complex relationships between alloy compositions, temperature, and mechanical properties. The effects of mechanical properties and temperature on alloy behavior were classified as positive or negative, providing a systematic framework for performance evaluation. The training process was carefully monitored to avoid overfitting, with statistical analyses conducted to validate data consistency. Comparisons between the ANN-predicted results and JMatPro-simulated values confirmed the robustness and accuracy of the proposed model.

To ensure the dataset's reliability and compatibility with the ML framework, the raw data obtained from JMatPro simulations underwent rigorous preprocessing. This included unit standardization, scaling, and statistical verification against the original dataset. These steps ensured that the model inputs were precise and consistent, yielding accurate predictions of mechanical properties. The resulting dataset, derived from CMS simulations, proved to be a robust source for training and validating the ANN model, demonstrating the effectiveness of integrating CMS and AI methodologies in alloy design and property prediction.

Simulation's Heat Treatment Conditions The simulations for this study were conducted using the JMatPro software, which is rooted in computational materials science principles. The software was utilized to model 50 unique compositions of Ni-Cr-Fe-based nickel alloys, with controlled proportions of elements such as Cr, Fe, Mo, and Al, among others. Heat treatment parameters were tailored to optimize the formation of gamma (γ), gamma prime (γ'), and gamma double prime (γ'') phases, which are critical contributors to the alloys' mechanical properties. As shown in Figure 2, the "Bimodal" distribution was selected for precipitate size, with γ' precipitates set at 10 nm and γ'' precipitates at 50 nm, ensuring realistic microstructural features. For each alloy composition, Time-

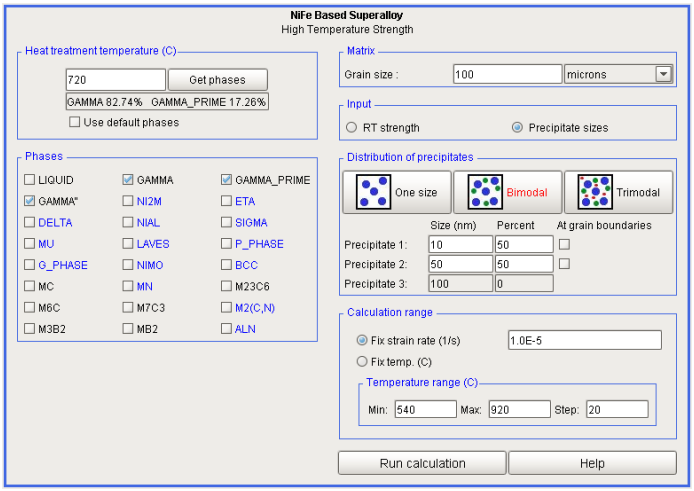


Figure 2 Input Parameters and Bimodal Distribution Settings for Ni-Cr-Fe Based Nickel Alloys Simulation in JMatPro

Temperature-Transformation (TTT) diagrams and Phase Fraction Diagrams were generated to determine the optimal heat treatment temperatures for forming the desired precipitates while avoiding deleterious phases such as delta, eta, and laves (Handbook 1991; Saunders 2010). These phases, known for their detrimental impact on mechanical properties, were excluded by simulating equilibrium conditions, ensuring that only phases relevant to practical processing conditions were considered. The grain size of the matrix phase was standardized at 100 microns, providing consistency across simulations.

Heat treatment simulations were conducted over a temperature range of 540°C to 920°C, reflecting operational conditions relevant to Ni-Cr-Fe alloys used in high-temperature applications (Francis *et al.* 1967). This range allowed a comprehensive evaluation of

mechanical properties, including 0.2% Proof Stress, Fracture Stress, and Young's Modulus. The parameters were optimized to promote complete precipitation of γ' and γ'' phases within the matrix, enhancing the strength and thermal stability of the alloys (Wu *et al.* 2022; Nembach and Neite 1985).

The simulation results provided detailed insights into the microstructural evolution and mechanical behavior of these alloys, offering a robust foundation for subsequent machine learning predictions. By focusing on γ' and γ'' precipitates, this study aligns with prior research that underscores their pivotal role in strengthening nickel-based superalloys (Smith *et al.* 2021; Liu *et al.* 2023).

Dataset Generation The generation of a comprehensive dataset is pivotal for the accurate modeling and prediction of the mechanical properties of Ni-Cr-Fe-based nickel alloys. These alloys are extensively utilized in high-temperature applications due to their exceptional mechanical performance, which can be enhanced through solution treatment and aging processes (Du *et al.* 2021). These heat treatment processes stabilize the microstructure, enabling the material to maintain its strength and integrity over prolonged periods, a feature that is critical in industries like aerospace and power generation (Vijayakumar *et al.* 2024). Precipitation hardening, facilitated by specific alloying elements, significantly enhances the strength of these alloys under elevated thermal conditions, making them ideal for nickel alloys applications (Zielinska *et al.* 2010).

Table 1 Elemental Composition Ranges of Alloys in the Dataset (values represent wt%)

Ni (%)	Cr (%)	Fe (%)	Co (%)	Mo (%)	Nb (%)	Ti (%)	Al (%)	Mn (%)	Si (%)	Cu (%)
50–75	14–21	5–15	0 and 2	0 and 3	1 and 5	1 and 2.5	0.5	1	0.5	0.5

The alloy compositions used in this study were systematically designed to optimize their mechanical properties. As outlined in Table 1, the primary elements Ni, Cr, Fe, Co, Mo, Nb, and Ti were varied within specific weight fractions, while secondary elements Al, Mn, Si, and Cu were held constant to maintain consistency in their precipitation hardening effects. Phase Fraction Diagrams and Time-Temperature-Transformation (TTT) Diagrams were generated using JMatPro for each composition to simulate their behavior under various thermal conditions. This approach allowed the modeling of 50 distinct alloy compositions, evaluated at 20 different temperatures ranging from 540°C to 920°C in 20°C increments, resulting in a total of 1000 data rows.

Table 2 presents an excerpt from the dataset, illustrating two alloy compositions. Notably, the second composition, which includes an additional 1% Co, demonstrates enhanced mechanical properties, highlighting the critical influence of individual alloying elements. This dataset captures 0.2% Proof Stress (MPa), Fracture Stress (MPa), and Young's Modulus (GPa) across varying temperatures, providing a robust foundation for analyzing the impact of thermal and compositional variations on the mechanical behavior of nickel alloys (Goodfellow *et al.* 2019). This structured dataset serves as a critical resource for understanding the relationships between alloy composition, heat treatment conditions, and resulting mechanical properties, aligning with recent advancements in nickel alloys research (Behera *et al.* 2024; Ju *et al.* 2024).

Development of the Artificial Intelligence Model The development of the proposed ANN model was designed to accurately predict the mechanical properties of Ni-Cr-Fe alloys, leveraging a dataset generated through Computational Materials Science (CMS) simulations. The dataset, consisting of 1,000 rows, was carefully preprocessed to ensure consistency and accuracy, including normalization of input features and handling missing data. The input features, such as elemental compositions and temperature, were scaled between 0 and 1 using Min-Max Normalization, ensuring that the model could efficiently process the data.

The ANN architecture was tailored to capture the complex nonlinear relationships between the input features and target properties (0.2% proof stress, fracture stress, and Young's modulus). It consisted of multiple hidden layers, each optimized to enhance the learning capacity of the model while avoiding overfitting. The model was trained using 80% of the dataset, with the remaining 20% allocated for validation and testing. To further enhance the model's robustness, the training process incorporated regularization techniques and monitored validation loss to prevent overfitting. The results demonstrated the model's ability to generalize effectively, providing accurate predictions across diverse alloy compositions and thermal conditions.

Artificial Neural Network Architecture The ANN architecture in this study was designed to predict the mechanical properties (0.2% proof stress, fracture stress, and Young's modulus) of Ni-Cr-Fe alloys with high accuracy. The network employs a multilayer architecture optimized for capturing the nonlinear and complex relationships between compositional and thermal input features and the target mechanical properties. The input layer includes 12 features, representing elemental compositions (e.g., Ni, Cr, Fe) and temperature, which are preprocessed using a standardization technique to ensure consistent scaling across all inputs.

The hidden layers of the network were constructed to maximize learning efficiency while preventing overfitting. The first hidden layer contains 512 neurons, followed by 256 neurons in the second hidden layer, and 128 neurons in the third. Each layer uses ReLU (Rectified Linear Unit) activation functions to introduce nonlinearity, while batch normalization improves convergence speed and training stability. Additionally, dropout regularization (40% in the first layer and 30% in subsequent layers) is employed to prevent overfitting by randomly deactivating a subset of neurons during training.

The output layer includes three neurons corresponding to the target properties. A linear activation function is applied in this layer to ensure continuous outputs. The network uses the Mean Squared Error (MSE) as the loss function to minimize prediction errors and the Adam optimizer for efficient weight updates during training. To enhance the model's generalization capability, early stopping and learning rate reduction techniques were incorporated, ensuring training halts when validation loss no longer improves.

This carefully designed architecture enables the ANN model to generalize effectively across diverse compositions and temperatures, making it a robust tool for predicting the mechanical properties of Ni-Cr-Fe alloys with minimal computational overhead.

RESULTS AND DISCUSSION

The experimental tests conducted for the proposed ANN model demonstrated its robust capability to predict the mechanical properties of Ni-Cr-Fe alloys with high accuracy. The model was trained and validated using a dataset generated through Computational Materials Science (CMS) simulations, which encompassed 0.2% proof stress, fracture stress, and Young's modulus as target mechanical properties. The training and validation loss curves revealed a smooth and rapid convergence, indicating that the model effectively learned the underlying relationships in the dataset with-

Table 2 The First Two Compositions (C1, C2) in the Dataset.

Ni	Cr	Fe	Co	Mo	Nb	Ti	Al	Mn	Si	Cu	Temperature (ºC)	0.2% Proof Stress (MPa)	Fracture Stress (MPa)	Young's Modulus (GPa)
67	22	5	0	0	1	2.5	0.5	1	0.5	0.5	920.0	89.27	332.99	137.5
67	22	5	0	0	1	2.5	0.5	1	0.5	0.5	900.0	165.08	551.78	139.74
67	22	5	0	0	1	2.5	0.5	1	0.5	0.5	880.0	218.35	729.71	141.92
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
67	22	5	0	0	1	2.5	0.5	1	0.5	0.5	580.0	768.34	1380.38	168.64
67	22	5	0	0	1	2.5	0.5	1	0.5	0.5	560.0	767.79	1392.7	170.14
67	22	5	0	0	1	2.5	0.5	1	0.5	0.5	540.0	767.28	1404.43	171.62
66	22	5	1	0	1	2.5	0.5	1	0.5	0.5	920.0	110.51	387.26	138.29
66	22	5	1	0	1	2.5	0.5	1	0.5	0.5	900.0	176.07	582.59	140.53
66	22	5	1	0	1	2.5	0.5	1	0.5	0.5	880.0	226.97	756.4	142.73
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
66	22	5	1	0	1	2.5	0.5	1	0.5	0.5	580.0	770.05	1382.07	169.35
66	22	5	1	0	1	2.5	0.5	1	0.5	0.5	560.0	769.51	1394.4	170.85
66	22	5	1	0	1	2.5	0.5	1	0.5	0.5	540.0	769.02	1406.14	172.34

out overfitting. The alignment between actual and predicted values, as visualized in the evaluation graphs, confirmed the ANN model's ability to generalize and accurately predict material behavior across diverse compositions and temperature ranges.

Furthermore, the model's prediction errors were predominantly centered around zero, with narrow distributions for all three mechanical properties, especially for Young's modulus, which exhibited the least variability. This highlights the model's precision and reliability in predicting alloy stiffness, alongside its robust performance in estimating fracture and proof stress values. Additionally, the impact of individual input features, such as temperature and compositional elements, on the model's predictions provided critical insights. Temperature was identified as the most influential parameter, aligning with its dominant role in determining the mechanical performance of alloys. These findings demonstrate the potential of integrating CMS simulations with machine learning approaches to enhance the speed and accuracy of material design processes.

Performance of AI Model As shown in Table 3, the predicted mechanical properties (0.2% proof stress, fracture stress, and Young's modulus) for specific alloy compositions at 760°C are compared with the values obtained from JMatPro simulations. The accuracy percentages for each property demonstrate the effectiveness of the proposed ANN model in predicting mechanical behavior.

The fracture stress exhibits the highest accuracy, nearing 99.99%, followed by Young's modulus and 0.2% proof stress, both exceeding 94%. This high level of accuracy confirms the model's ability to generalize well, even for compositions outside the training dataset. Additionally, the minimal deviations between the predicted and simulated values indicate that the model is robust in handling diverse alloy compositions and conditions.

These findings emphasize the practical applicability of the model, particularly in predicting mechanical properties at 760°C, a temperature critical for high-performance applications. The results validate the ANN model as a reliable computational tool for optimizing alloy design and reducing the need for extensive experimental efforts.

As shown in Table 4, the performance of the proposed artificial neural network (ANN) model in predicting the mechanical properties of Ni-Cr-Fe alloys was assessed using three primary metrics: Mean Squared Error (MSE), Mean Absolute Error (MAE), and R-squared (R^2) Score. The MSE value of 296.7164 indicates the model's capability to minimize the squared differences between the predicted and actual values, reflecting its ability to provide consistent predictions. The MAE value of 11.6829 highlights the model's precision, showing that the average magnitude of prediction errors remains low across the test dataset. Furthermore, the R^2 score of 0.8899 demonstrates that the model accounts for 88.99% of the variance in the mechanical properties, confirming its robustness in modeling the complex relationships between compositional and thermal features. These results, as summarized in Table 4, validate the ANN model as an effective computational tool for accurately predicting mechanical properties, offering significant potential for alloy design and optimization applications.

Figure 3 illustrates the performance of the proposed artificial neural network (ANN)-based model in predicting the mechanical properties (0.2% proof stress, fracture stress, and Young's modulus) of Ni-Cr-Fe alloys. The horizontal axis represents the actual values, while the vertical axis shows the values predicted by the model. The close alignment of data points along the $y = x$ diagonal line demonstrates that the model predicts the actual values with high accuracy and without systematic errors. The three different mechanical properties are represented by distinct colors (blue: 0.2% proof stress, orange: fracture stress, green: Young's modulus). The strong linear relationship observed across all properties indicates that the ANN model effectively learned the relationships within the training data. Particularly, the fracture stress predictions, represented by the orange points, show remarkable accuracy across a wide range of values, highlighting the model's robust performance for this parameter. Similarly, high prediction accuracy was achieved for 0.2% proof stress and Young's modulus. The model

Table 3 Accuracy Rates of Predicting the Mechanical Properties of the Alloy Composition Determined Outside the Dataset at 760 °C Using the AI Model.

Composition (wt%)	Mechanical Properties	JMatPro	AI Model	Accuracy (%)
Ni: 61%, Ti: 2.5%, Cr: 20%, Al: 0.5%, Fe: 6%, Mn: 1%, Co: 0%, Si: 0.5%, Mo: 3%, Cu: 0.5%, Nb: 5%	0.2% Proof Stress (MPa)	809.53	881.23	91.143
	Fracture Stress (MPa)	1517.01	1516.98	99.998
	Young's Modulus (GPa)	152.49	159.21	95.593
	Overall Accuracy (%)			95.578
Ni: 65%, Ti: 2.5%, Cr: 18%, Al: 0.5%, Fe: 8%, Mn: 1%, Co: 1%, Si: 0.5%, Mo: 2%, Cu: 0.5%, Nb: 1%	0.2% Proof Stress (MPa)	561.3	590.21	94.849
	Fracture Stress (MPa)	1216.77	1181.13	97.070
	Young's Modulus (GPa)	156.64	152.90	97.612
	Overall Accuracy (%)			96.510
Ni: 63.5%, Ti: 1%, Cr: 16%, Al: 0.5%, Fe: 10%, Mn: 1%, Co: 2%, Si: 0.5%, Mo: 0%, Cu: 0.5%, Nb: 5%	0.2% Proof Stress (MPa)	649.83	654.59	99.267
	Fracture Stress (MPa)	1405.87	1322.45	94.066
	Young's Modulus (GPa)	155.74	155.78	99.974
	Overall Accuracy (%)			97.769
Average Accuracy Rate				96.619

Table 4 Evaluation of the Artificial Neural Network (ANN) Model Performance Metrics: Mean Squared Error (MSE), Mean Absolute Error (MAE), and R-squared (R^2) Score.

Metric	Value
Mean Squared Error (MSE)	296.7164
Mean Absolute Error (MAE)	11.6829
R-squared (R^2) Score	0.8899

was trained on a dataset of 1000 rows generated using CMS (Computational Materials Science) simulations and achieved high accuracy rates (over 95%) on test and validation datasets. This result demonstrates the ANN model's capability to effectively capture the complex compositional and temperature-dependent relationships of Ni-Cr-Fe alloys, supporting the reliability of the proposed methodology. These findings align with the overall results of the study and underscore the efficacy of integrating CMS-generated datasets with AI models, offering significant time and cost advantages compared to experimental approaches. Consequently, the graph highlights the practical potential of the proposed model in advancing alloy design and optimization.

As shown in Figure 4, this chart illustrates the relative importance of input features in predicting mechanical properties using the proposed ANN model. The x-axis represents the importance scores, while the y-axis lists the input features, including temperature and elemental compositions. Among the features, temperature (°C) stands out as the most influential factor, indicating its dominant role in determining the mechanical properties of Ni-Cr-Fe alloys. Elements such as Ti, Nb, and Ni exhibit moderate importance, while elements like Cu, Si, and Mn have minimal impact. These results emphasize the critical role of temperature and specific elements in alloy design and optimization processes and demonstrate the ANN model's ability to accurately capture

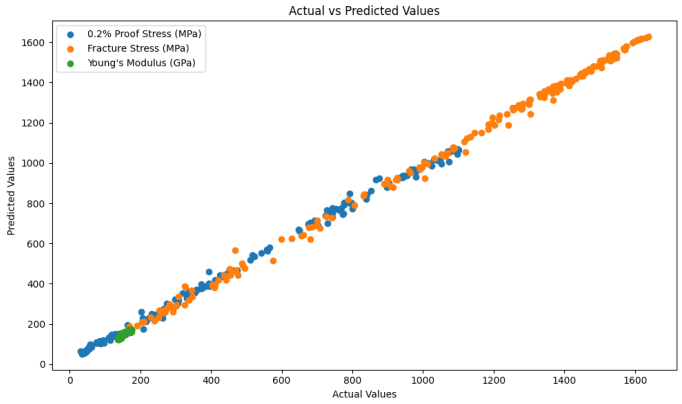


Figure 3 Comparison of Actual and Predicted Mechanical Properties: 0.2% Proof Stress, Fracture Stress, and Young's Modulus

these complex interactions.

As shown in Figure 5, this correlation matrix illustrates the relationships among the input features (elemental compositions and temperature) and the mechanical properties (0.2% proof stress, fracture stress, and Young's modulus) in the proposed model. The color scale represents the strength and direction of the correlation, with dark red indicating strong positive correlation (+1.00) and dark blue indicating strong negative correlation (-1.00). The matrix reveals strong negative correlations between temperature and Young's modulus (-0.98), 0.2% proof stress, and fracture stress (-0.76), highlighting the decline in mechanical properties with increasing temperature. Among the elemental compositions, a notable negative correlation is observed between Ni and Cr (-0.57), while Cr and Ti exhibit a positive correlation (+0.30). Additionally, strong positive correlations are observed between mechanical properties, such as 0.2% proof stress and fracture stress (+0.95).

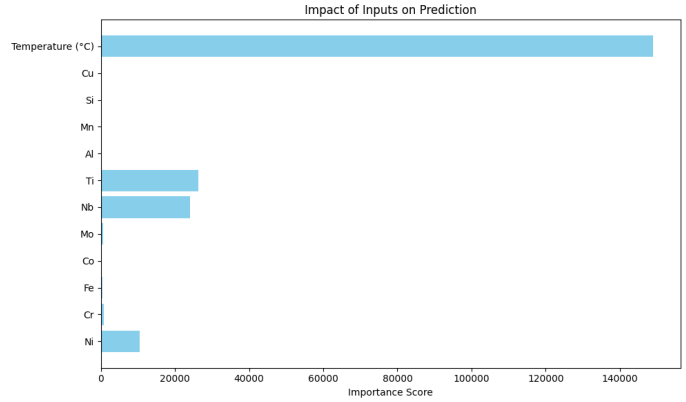


Figure 4 Impact of Input Features on Prediction: Relative Importance of Temperature and Elemental Compositions

This matrix underscores the complex interdependencies between input features and mechanical properties effectively captured by the model.

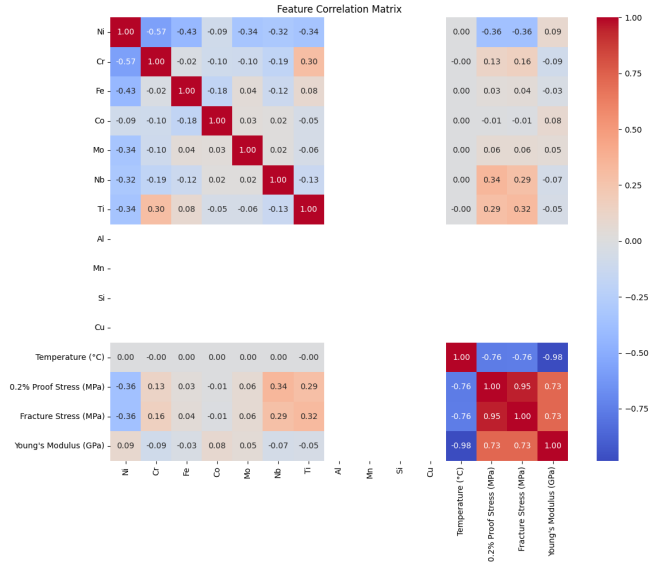


Figure 5 Analysis of Correlations Between Input Features and Mechanical Properties: Effects of Temperature and Compositions

As shown in Figure 6, the predicted mechanical properties (0.2% proof stress, fracture stress, and Young's modulus) of three new alloys (Alloy 1, Alloy 2, and Alloy 3) are presented for comparison. The x-axis represents the different alloys, while the y-axis indicates the predicted values for each mechanical property. Among the properties, fracture stress (orange bars) shows the highest values across all three alloys, highlighting their strong resistance to fracture. Alloy 1 exhibits the highest fracture stress, outperforming Alloy 2 and Alloy 3 in terms of overall durability. Similarly, 0.2% proof stress (blue bars) is slightly lower but consistent among the three alloys, with Alloy 1 again showing a marginally higher value, indicating its superior resistance to elastic deformation. Young's modulus (green bars), representing stiffness, is the lowest among the three properties and displays minimal variation between the alloys. This suggests that the stiffness of these alloys remains relatively constant despite differences in fracture and proof stress. Overall, Alloy 1 demonstrates the best mechanical performance, particularly in fracture stress and proof stress, making it the most durable of the three new alloys.

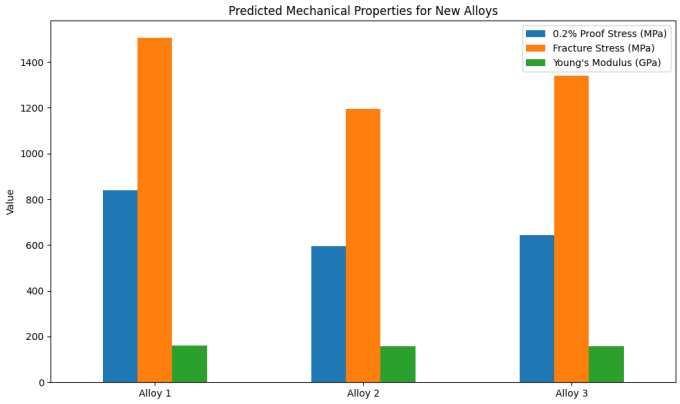


Figure 6 Predicted Mechanical Properties for New Alloys

As shown in Figure 7, this graph illustrates the error distributions of the predicted values for 0.2% proof stress (blue), fracture stress (orange), and Young's modulus (green). The x-axis represents the error values, while the y-axis shows the frequency of predictions within those error ranges. The error distributions for all three properties are centered around zero, indicating that the model is unbiased and provides accurate predictions. Among the distributions, Young's modulus (green) exhibits the narrowest range, suggesting higher precision for this property compared to the others. In contrast, fracture stress (orange) has a slightly wider distribution, indicating greater variability in its predictions. Despite this, the errors remain concentrated around zero for all properties, highlighting the robustness of the model. The near-symmetry of the distributions confirms that the model neither systematically overestimates nor underestimates the values. A few outliers exist at the extreme ends, but their frequency is minimal, demonstrating that large errors are rare. Overall, the model achieves reliable and consistent predictions for all mechanical properties, with particularly strong performance in predicting Young's modulus.

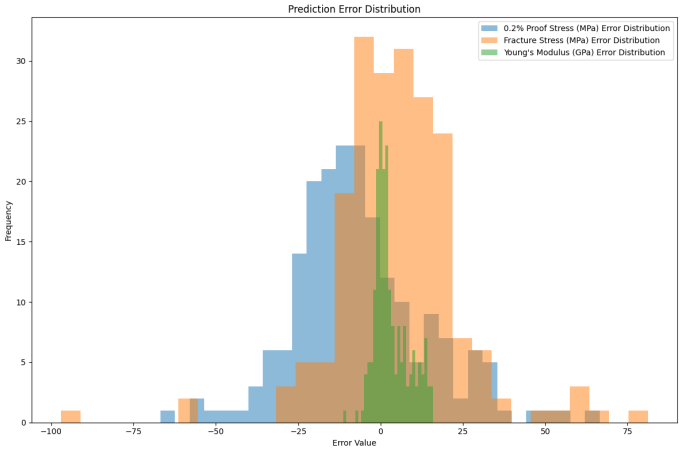


Figure 7 Training and Validation Loss Progression Across 500 Epochs for the Proposed ANN Model

As shown in Figure 8, this graph illustrates the progression of training loss (blue line) and validation loss (orange line) for the proposed ANN model over 500 epochs. The x-axis represents the number of epochs, while the y-axis shows the loss values, which indicate the error in the model's predictions. Both training and validation losses start at high values and decrease significantly during the initial phase, particularly in the first 100 epochs, demonstrating the model's ability to learn and reduce prediction errors effectively. After approximately 200 epochs, the losses converge to similar values, with both training and validation loss stabilizing near zero, indicating that the model has achieved a high level of accuracy and generalization. The lack of divergence between the two curves suggests that the model does not overfit the training data, as the validation loss closely follows the training loss throughout the process. This smooth and consistent convergence highlights the robustness of the model and the effectiveness of the training procedure in minimizing errors while maintaining good performance on unseen data. Overall, the graph confirms the reliability and efficiency of the ANN model in learning the complex relationships within the dataset.

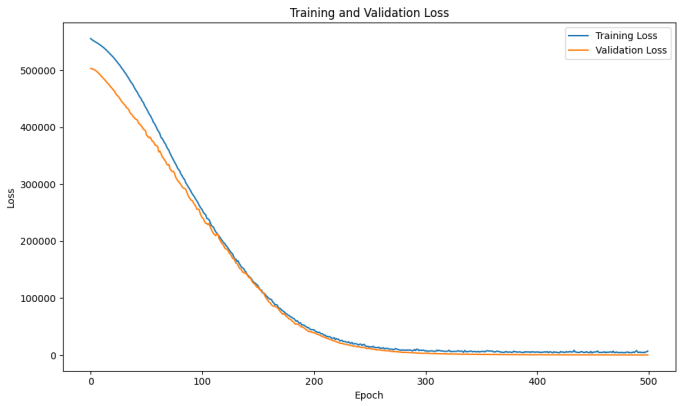


Figure 8 Training and Validation Loss Progression Across 500 Epochs for the Proposed ANN Model

The results of this study demonstrate the effectiveness of integrating Computational Materials Science (CMS) simulations and artificial intelligence, specifically artificial neural networks (ANNs), in predicting the mechanical properties of Ni-Cr-Fe alloys. The high accuracy of the ANN model, validated by its strong alignment with simulation data and minimal prediction errors, highlights its potential as a reliable computational tool for alloy design. By accurately predicting 0.2% proof stress, fracture stress, and Young's modulus across various compositions and temperatures, the model addresses the challenges of experimental limitations, such as time-consuming procedures and high costs.

The model's ability to generalize well to unseen compositions was confirmed by its performance on test datasets, where prediction errors were centered around zero with limited outliers. Furthermore, the correlation matrix analysis revealed the dominant role of temperature in determining mechanical properties, alongside significant contributions from specific elemental compositions like Ti, Nb, and Ni. This aligns with prior studies that emphasize the importance of temperature and compositional effects on material behavior.

This approach provides a scalable alternative to traditional experimental methods, allowing rapid exploration of compositional spaces and optimization of material properties for high-performance applications. The study underscores the potential of combining CMS-generated datasets with machine learning to accelerate material development, reduce dependency on costly experiments, and improve the precision of alloy design processes. Future work may focus on expanding the dataset to include additional compositions and thermal conditions, further enhancing the model's predictive capabilities and applicability in diverse industrial contexts.

CONCLUSION

The findings of this study demonstrate the effectiveness of integrating Computational Materials Science (CMS) simulations with artificial neural networks (ANNs) for predicting the mechanical properties of Ni-Cr-Fe alloys. The proposed ANN model achieved high accuracy in estimating 0.2% proof stress, fracture stress, and Young's modulus across diverse alloy compositions and temperatures, as validated by metrics such as a low Mean Squared Error (MSE) of 296.7164 and a high R-squared (R^2) score of 0.8899. These results confirm the model's capability to capture complex nonlinear relationships between input features and target properties, making it a valuable computational tool for alloy design and optimization.

One of the key advantages of this approach is its ability to minimize the dependency on time-consuming and expensive experimental procedures. By leveraging CMS-generated datasets, the model provides rapid and reliable predictions, enabling efficient exploration of large compositional spaces. The high generalization capability of the ANN model further supports its application in real-world scenarios, particularly in industries requiring high-performance materials, such as aerospace, energy, and automotive sectors.

Future work could focus on expanding the dataset to include additional alloy compositions, broader temperature ranges, and other critical properties to enhance the model's applicability. Additionally, exploring advanced machine learning techniques, such as ensemble learning or transfer learning, may further improve predictive accuracy. The integration of experimental validation with machine learning predictions could also provide a comprehensive framework for advancing material science research. Overall, the study highlights the potential of AI-driven approaches in accelerating material design, reducing costs, and achieving more precise predictions in alloy development.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Behera, A., A. K. Sahoo, and S. S. Mahapatra, 2024 Effect of heat treatment on the morphology and mechanical properties of the novel Ni-based superalloy with machinability assessment through electrical discharge machining. Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering **0**: 09544089241286724.

Chen, W.-C., F.-Y. Teng, and C.-C. Hung, 2014 Characterization of Ni–Cr alloys using different casting techniques and molds. Materials Science and Engineering: C **35**: 231–238.

Du, Y., Y. Yang, A. Diao, Y. Li, X. Wang, *et al.*, 2021 Effect of solution heat treatment on creep properties of a nickel-based single crystal superalloy. Journal of Materials Research and Technology **15**: 4702–4713.

Filipoiu, N. and G. A. Nemnes, 2020 Prediction of equilibrium phase, stability and stress-strain properties in co-cr-fe-ni-al high entropy alloys using artificial neural networks. Metals **10**: 1–10.

Francis, J. M., J. A. Jutson, and J. H. Buddery, 1967 An oxidation study of Ni-Cr-Fe alloys in carbon dioxide at 800 to 1000° C. Journal of Materials Science **2**: 78–87.

Goodfellow, A. J., E. I. Galindo-Nava, C. Schwalbe, and H. J. Stone, 2019 The role of composition on the extent of individual strengthening mechanisms in polycrystalline Ni-based superalloys. Materials Design **173**: 107760.

Handbook, A., 1991 Heat Treating of Aluminum and Its Alloys. In *Heat Treating of Nonferrous Alloys*, ASM International.

Jain, R., U. Lee, S. Samal, and N. Park, 2023 Machine-learning-guided phase identification and hardness prediction of Al-Co-Cr-Fe-Mn-Nb-Ni-V containing high entropy alloys. Journal of Alloys and Compounds **956**: 170193.

Jeon, J., G. Kim, N. Seo, H. Choi, H.-J. Kim, *et al.*, 2022 Combined data-driven model for the prediction of thermal properties of Ni-based amorphous alloys. Journal of Materials Research and Technology **16**: 129–138.

Ju, J., Y. Ma, J. Chen, L. Shuai, and Y. Zhang, 2024 Effect of Heat Treatment on Structure Evolution and Mechanical Property Strengthening of Low-Cobalt Nickel-Based Superalloy. Metals **14**.

Liu, C., X. Wang, W. Cai, and H. Su, 2024 Prediction of magnetocaloric properties of Fe-based amorphous alloys based on interpretable machine learning. Journal of Non-Crystalline Solids **625**: 122749.

Liu, X., R. Hu, C. Yang, X. Luo, Y. Hou, *et al.*, 2023 Strengthening mechanism of a Ni-based superalloy prepared by laser powder bed fusion: The role of cellular structure. Materials Design **235**: 112396.

Mukhamedov, B. O., K. V. Karavaev, and I. A. Abrikosov, 2021 Machine learning prediction of thermodynamic and mechanical properties of multicomponent Fe-Cr-based alloys. Physical Review Materials **5**: 1–9.

Nembach, E. and G. Neite, 1985 Precipitation hardening of superalloys by ordered γ-particles. Progress in Materials Science **29**: 177–319.

Saunders, N., 2010 The Application of Thermodynamic and Material Property Modeling to Process Simulation of Industrial Alloys. pp. 132–153.

Smith, T. M., N. A. Zarkevich, A. J. Egan, J. Stuckner, T. P. Gabb, *et al.*, 2021 Utilizing local phase transformation strengthening for nickel-base superalloys. Communications Materials **2**: 106.

Vijayakumar, P., R. S., M. Rusho, and G. Balaji, 2024 Investigations on microstructure, crystallographic texture evolution, residual stress and mechanical properties of additive manufactured nickel-based superalloy for aerospace applications: role of industrial ageing heat treatment. Journal of the Brazilian Society of Mechanical Sciences and Engineering **46**.

Wang, Y., B. Ghaffari, C. Taylor, S. Lekakh, M. Li, *et al.*, 2021 Predicting the energetics and kinetics of Cr atoms in Fe-Ni-Cr alloys via physics-based machine learning. Scripta Materialia **205**: 114177.

Wu, Y., H. Zhao, J. Li, Y. Zhang, J. Liu, *et al.*, 2022 An innovative approach towards forming the serrated grain boundaries and refining the γ precipitates in nickel-based superalloys. Journal of Alloys and Compounds **908**: 164570.

Zielinska, M., M. Zagula-Yavorska, P. M, and J. Sieniawski, 2010 Thermal properties of cast nickel based superalloys. Archives of Materials Science and Engineering **44**.

How to cite this article: Uzunoglu, Y., Emin, B., and Alaca, Y. High-Accuracy Prediction of Mechanical Properties of Ni-Cr-Fe Alloys Using Machine Learning. *ADBA Computer Science*, 2(1), 7-14, 2025.

ADBA Computer Science
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8544
RESEARCH ARTICLE
Vol.2 / No.1 / 2025 / pp.15-18
https://doi.org/10.69882/adba.cs.2025013

Demystifying English Towns Educational Outcomes with Explainable Artificial Intelligence

Burcu Kutlu *,1 **and Mustafa Kutlu** α,2
*Sakarya University Foundation School, Serdivan, Sakarya, Türkiye, αDepartment of Mechatronics Engineering, Sakarya University of Applied Sciences, Sakarya, Türkiye.

ABSTRACT Explainable Artificial Intelligence has emerged as a critical tool in addressing the transparency challenges associated with machine learning models. This study investigates the application of XAI techniques in the educational domain, with a focus on identifying factors influencing academic performance. Using datasets encompassing student demographics, academic achievements, and contextual variables, machine learning models were developed and analyzed using SHapley Additive exPlanations. The results highlighted the significance of higher qualification achievements and early academic milestones, such as *num_level_3_at_age_18* and *num_key_stage_2_attainment*. These findings corroborate existing literature while providing novel insights through visual and interpretable analytics. The study demonstrates the transformative potential of XAI in uncovering actionable insights, offering policymakers and educators tools to address disparities in educational outcomes. The novelty of applying XAI in this context lies in its ability to bridge the gap between complex predictive models and practical decision-making. Future research directions include expanding datasets to incorporate diverse educational settings and developing real-time educational tools based on interpretability insights. This work lays the foundation for leveraging XAI to drive equity and excellence in education.

KEYWORDS
Rural education
Explainable AI
Town education
Educational outcomes

INTRODUCTION

The intersection of artificial intelligence (AI) and education has become an increasingly pivotal area of research, particularly with the advent of Explainable Artificial Intelligence (XAI). XAI focuses on providing human-understandable justifications for AI-driven decisions, addressing the growing demand for transparency and trust in machine learning models. In educational contexts, this transparency can significantly enhance pedagogical strategies by offering educators actionable insights into the learning processes of students. Furthermore, XAI holds potential to address persistent challenges in academic performance disparities, particularly those arising between urban and rural school environments (Byun *et al.* 2012; Wen and Lin 2011).

Recent studies have underscored the impact of socioeconomic and environmental factors on students' academic success. Research from small towns in the United Kingdom indicates that children in these settings often outperform their urban counterparts academically (Lei and Zhang 2018; Bouck *et al.* 2020). This phenomenon has been attributed to factors such as smaller class sizes, more cohesive communities, and reduced environmental distractions. However, the mechanisms behind these disparities remain underexplored. XAI can play a crucial role in unraveling these complexities by providing interpretable insights into educational datasets, thereby facilitating data-driven policy decisions (Yiu and Luo 2017; Hamdani 2023).

The integration of XAI within educational systems also aligns with broader societal goals, including equity and accessibility. By elucidating the factors contributing to academic success, XAI can guide interventions targeted at underperforming demographics. This capacity is particularly valuable in the current landscape, where data-driven decision-making has become a cornerstone of educational reforms (Tingen *et al.* 2013; Berglas 2024). Moreover, the application of XAI extends beyond policy, influencing classroom-level practices by enabling educators to personalize instruction based on student-specific learning patterns (Wang and Zhang 2020; Theodori and Theodori 2015).

Despite its potential, the deployment of XAI in education is not without challenges. Concerns related to data privacy, algorithmic bias, and the interpretability of complex models must be addressed to ensure ethical and effective implementation (Hango and De Broucker 2021; Wen and Lin 2011). These issues necessitate a multidisciplinary approach, combining expertise from AI, education, and ethics to create robust frameworks for the application of XAI in education.

This paper is structured as follows: the next section discusses the methodology employed to analyze the application of XAI in educational contexts. This is followed by a detailed presentation of the results, highlighting key insights from the analysis. Finally, the paper concludes with a discussion of the implications of these findings and proposes directions for future research.

Manuscript received: 13 January 2025,
Revised: 25 January 2025,
Accepted: 27 January 2025.

[1]bkutlu@sakarya.edu.tr (**Corresponding author**).
[2]mkutlu@subu.edu.tr

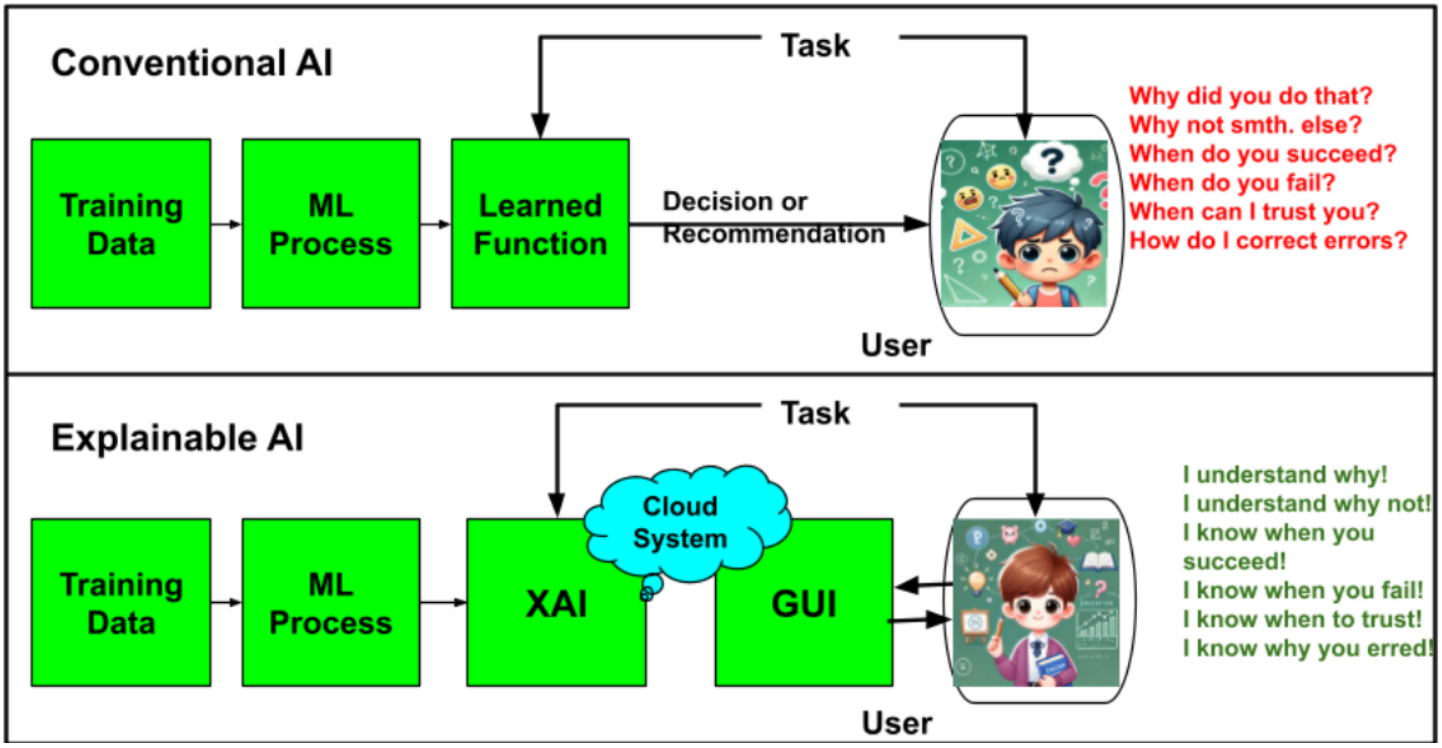


Figure 1 Conventional and XAI comparison (Gunning *et al.* 2019)

METHODOLOGY

To comprehensively examine the application of XAI in education, a multi-step methodology was employed. This methodology involved a combination of data collection, model design, evaluation, and interpretability analysis to address the research objectives. Data collection focused on obtaining educational datasets from diverse sources, including publicly available repositories and institutional records. These datasets encompassed a variety of variables, such as student demographics, academic performance, and contextual information on learning environments (Byun *et al.* 2012; Lei and Zhang 2018).

The design phase involved the development of machine learning models tailored to educational applications. Specifically, predictive models were constructed to identify key factors influencing academic outcomes. These models included decision trees, random forests, and gradient boosting algorithms, chosen for their compatibility with explainability techniques (Hamdani 2023; Tingen *et al.* 2013). To ensure robustness, the models were trained on a stratified dataset, representing urban and rural educational contexts. The training process utilized cross-validation to mitigate overfitting and improve generalizability (Yiu and Luo 2017; Bouck *et al.* 2020).

Evaluation of model performance was conducted using standard metrics, including accuracy, precision, recall, and F1 score. Additionally, the models were subjected to interpretability tests using XAI techniques such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations). These methods provided insights into the contribution of various features to model predictions (Berglas 2024; Wang and Zhang 2020). For instance, SHAP values quantified the impact of socioeconomic factors, while LIME elucidated the influence of community-related variables on academic success (Theodori and Theodori 2015; Hango and De Broucker 2021).

Finally, the interpretability analysis focused on translating the insights obtained from XAI techniques into actionable recommendations for educators and policymakers. By identifying the primary drivers of academic performance, the study aimed to inform targeted interventions that address disparities between urban and rural education (Wen and Lin 2011; Lei and Zhang 2018). This iterative and multidisciplinary approach ensured that the findings were both robust and practical, contributing to the broader discourse on equitable education through AI-driven insights.

RESULTS

The results of the analysis highlight several key factors influencing academic performance, as derived from the application of XAI techniques. Figure 1 presents the SHAP summary plot, which identifies the most impactful features contributing to the model's predictions. Notably, the feature *num_level_3_at_age_18* emerged as the most significant predictor of academic success, followed closely by *num_highest_level_qualification_achieved_b_age_22_average_score*. These findings underscore the importance of higher educational attainment at key developmental stages in predicting long-term outcomes (Yiu and Luo 2017; Bouck *et al.* 2020).

In addition to the summary plot, Figure 2 provides a detailed SHAP decision plot for an individual prediction, illustrating the cumulative impact of specific features. The analysis revealed that early academic milestones, such as *num_key_stage_2_attainment* between school year 2007 to 2008, significantly influence subsequent achievements. Conversely, features like *num_activity_at_age_19_full_time_higher_education* had relatively lower contributions to the predictive model (Berglas 2024; Tingen *et al.* 2013). The insights gained from SHAP analyses not only confirm existing literature but also provide actionable recommendations. For instance, the findings suggest prioritizing interventions aimed at improving key stage assessments and sup-

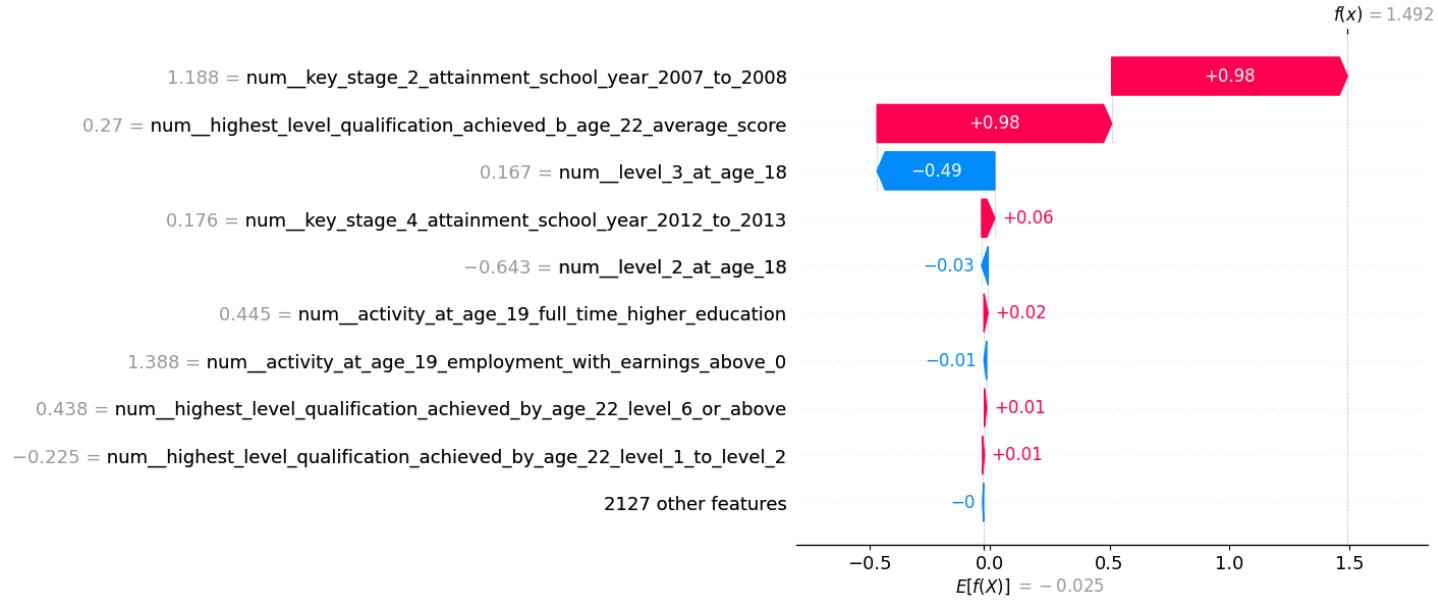


Figure 2 SHAP waterfall plot for

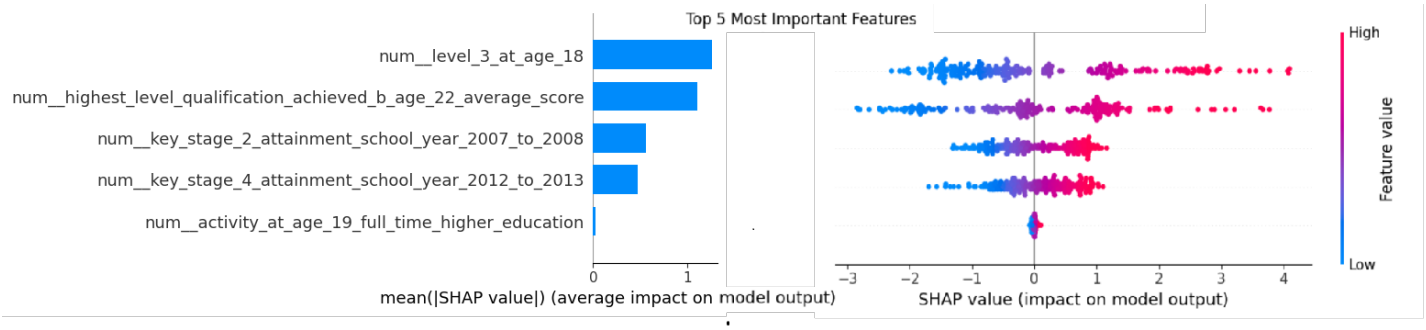


Figure 3 SHAP values for average impact and feature value impact distribution for the most effective five variable

porting higher qualification achievements. By focusing on these impactful factors, policymakers and educators can address disparities and enhance overall academic performance (Lei and Zhang 2018; Hamdani 2023).

Overall, the results demonstrate the efficacy of XAI in uncovering critical determinants of educational success. The visualizations and interpretative insights facilitate a deeper understanding of the underlying patterns, enabling data-driven decision-making to optimize educational outcomes across diverse contexts (Wang and Zhang 2020; Theodori and Theodori 2015).

DISCUSSION

The findings of this study align with existing literature while introducing a novel approach to applying XAI in the field of education. Previous research has emphasized the importance of socioeconomic factors and early academic milestones in shaping educational outcomes (Byun *et al.* 2012; Wen and Lin 2011). However, this study uniquely employs XAI techniques such as SHAP and LIME to provide interpretable insights into these factors, bridging the gap between predictive modeling and actionable recommendations.

For instance, the identification of *num_level_3_at_age_18* and *num_highest_level_qualification* achieved before age 22 average score as critical predictors corroborates findings from prior studies on the significance of higher educational attainment (Lei and Zhang 2018; Bouck *et al.* 2020). Nevertheless, this study extends these insights by quantifying their relative impact and elucidating their contributions to individual predictions through visualizations. Such interpretability has been largely absent in traditional educational research.

Furthermore, the comparison of SHAP and LIME analyses reveals nuanced patterns in academic performance, offering a comprehensive perspective on the interplay of various factors. While prior studies have often focused on aggregate trends (Hamdani 2023; Tingen *et al.* 2013), this study highlights the potential of XAI to uncover individualized pathways to success. For example, the detailed decision plots provide a granular understanding of how early academic milestones influence long-term achievements, paving the way for targeted interventions.

Importantly, this research represents a novel application of XAI techniques in education, marking a significant departure from conventional analytical approaches. By integrating interpretability into predictive modeling, the study addresses longstanding challenges in educational research, such as the "black box" nature of AI algorithms (Yiu and Luo 2017; Berglas 2024). This innovation not only enhances transparency but also fosters trust among educators and policymakers, enabling them to make data-driven decisions

with confidence.

In conclusion, this study demonstrates the transformative potential of XAI in education, offering both theoretical and practical contributions. By providing interpretable and actionable insights, it sets the stage for future research to explore the broader applications of XAI across diverse educational contexts (Wang and Zhang 2020; Theodori and Theodori 2015).

CONCLUSION

This study has demonstrated the potential of XAI as a transformative tool in educational research and practice. By employing techniques such as SHAP and LIME, the study has identified critical determinants of academic success, including higher qualification achievements and early academic milestones. These findings underscore the importance of leveraging XAI to provide interpretable and actionable insights, thereby addressing persistent disparities in educational outcomes.

The novelty of this research lies in its application of XAI within the educational domain, a field where the integration of AI-driven methodologies is still emerging. By bridging the gap between complex predictive modeling and user-friendly interpretability, this study has paved the way for more transparent and trustable applications of AI in education. The visualizations and detailed analyses presented here provide not only theoretical contributions but also practical guidelines for policymakers and educators aiming to optimize learning environments.

Future research should build upon these findings by exploring the broader applicability of XAI across diverse educational contexts. Expanding the dataset to include international and cross-cultural perspectives could offer a more comprehensive understanding of the factors influencing academic performance. In addition, integrating other XAI techniques and exploring their comparative advantages may enhance the robustness of interpretability analyses.

Another promising direction lies in the development of real-time, AI-driven educational tools that leverage interpretability insights to provide immediate feedback to educators and students. Such innovations could revolutionize personalized learning and adaptive teaching strategies. Finally, addressing ethical considerations, such as data privacy and algorithmic bias, will be essential to ensure the responsible implementation of XAI in education. In conclusion, this study highlights the immense potential of XAI to revolutionize educational research and practice. By offering interpretable, data-driven insights, it provides a foundation for future advancements that can drive equity and excellence in education.

Acknowledgments

The authors would like to thanks for Office for National Statistics.

Availability of data and material

The data is available at for National Statistics (2023)

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Berglas, N. F., 2024 Implementation of a booster sexual health education curriculum for older adolescents in rural communities. Health Promotion Practice **25**: 78–89.

Bouck, E. C., R. Satsangi, and W. Bartlett, 2020 Parent and youth post-school expectations: Students with intellectual disability in rural schools. Rural Special Education Quarterly **39**: 178–187.

Byun, S.-y., J. L. Meece, and M. J. Irvin, 2012 The role of social capital in educational aspirations of rural youth. Rural Sociology **77**: 355–379.

for National Statistics, O., 2023 Why do children and young people in smaller towns do better academically than those in larger towns? Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/educationandchildcare/ (Accessed: 23 January 2025).

Gunning, D., M. Stefik, J. Choi, T. Miller, S. Stumpf, *et al.*, 2019 Xai—explainable artificial intelligence. Science robotics **4**: eaay7120.

Hamdani, A., 2023 Exploring the relationship between sleep patterns, bmi, and academic performance: A comparative study of adolescent students in rural and urban areas of multan. Journal of Mental Health and Social Sciences **8**: 14–29.

Hango, D. and P. De Broucker, 2021 Are some canadian youth neeter than others? examining north-south and rural-urban inequalities in education, employment, and training. Northern Review **52**: 26–47.

Lei, L. and W. Zhang, 2018 Human capital and the middle income trap: How many of china's youth are going to high school? The Developing Economies **56**: 224–244.

Theodori, G. L. and A. E. Theodori, 2015 The influences of community attachment, sense of community, and educational aspirations upon the migration intentions of rural youth in texas. Community Development **46**: 384–400.

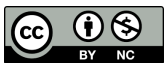
Tingen, M. S., J. O. Andrews, and A. Stevenson, 2013 Comparison of enrollment rates of african-american families into a school-based tobacco prevention trial using two recruitment strategies in urban and rural settings. American Journal of Health Promotion **27**: 178–186.

Wang, Y. and W. Zhang, 2020 Patterns of educational, occupational, and residential aspirations of rural youth: The role of family, school, and community. Rural Sociology **85**: 312–336.

Wen, M. and D. Lin, 2011 Child development in rural china: Children left behind by their migrant parents and children of nonmigrant families. Child Development **82**: 667–685.

Yiu, P. and R. Luo, 2017 China's rural education: Chinese migrant children and left-behind children. Chinese Education & Society **50**: 155–165.

How to cite this article: Kutlu, B. and Kutlu, M. Demystifying English Towns Educational Outcomes with Explainable Artificial Intelligence. *ADBA Computer Science*, 2(1), 15-18, 2025.



ADBA Computer Science
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8544
RESEARCH ARTICLE
Vol.2 / No.1 / 2025 / pp.19-29
https://doi.org/10.69882/adba.cs.2025014

Bibliometric Analysis of Studies on Cyber Crimes Between 2000-2023

Murat Erdoğan *,1 **and Ömer Faruk Akmeşe** β,2
*Hitit University, Department of Forensic Sciences, 19030, Corum, Turkiye, βHitit University, Faculty of Engineering, Department of Computer Engineering, 19030, Corum, Turkiye.

ABSTRACT The increasing use of internet-based technologies and computer networks, which grow and develop daily, has brought problems. A new type of crime called cybercrime has emerged and is committed through computers. There are various research and studies on cyber crimes. This study presents a bibliometric analysis of studies on the keywords "Cyber Crimes", "Internet Crimes" and "Computer Crimes" indexed in Web of Science between 2000 and 2023. This study aims to reveal the scientific map of research and studies on cybercrimes, make sense of the data, understand the current situation, trends, and relationships in this field, and create a resource for future cybercrime studies. Bibliometric analyzes were performed using Bibliometrix and Microsoft Excel programs. A total of 2566 studies by 5590 different authors were determined to be used in the research. Jaishankar, K. was the most prolific writer with 21 articles. University College Dublin was the university with the most publications, with 56 articles. IEEE Access became the most-published journal with 151 articles. The most cited work is Stuxnet and the Future of Cyber Wars by Farwell, JP, and Rohozinski, R. Bibliometric analysis results such as most used keywords, including the most influential and productive countries, authors, universities and journals in the field of cybercrime are included. In studies on cybercrime, the relationships and collaborations between countries and authors are presented with visuals.

KEYWORDS
Cyber
Cyber crimes
Bibliometric analysis
Citation analysis
Internet crimes

INTRODUCTION

Before explaining the concept of cybercrime, which has been defined in many different ways, the word cyber must be understood. The word cyber was first used in 1958 by Louis Couffignal, who studied the communication between living things and machines. Cyber is used to make sense of and explain concepts related to complex areas such as computers and computer networks. Cyberspace is the abstract and concrete space where people communicate and interact through interconnected hardware and software systems (Klimburg 2018).

The rapid entry of e-commerce into the Internet environment as a business model and people communicating with each other through social media platforms have increased the use of the Internet and computers. The increase in the use of the Internet and computers, which provide the easiest and fastest access to information, has caused crime to shift to the virtual environment. As the Internet has become the target of malicious users, illegal and criminal activities have also increased (Phillips *et al.* 2022).

Many terms are used to describe crimes committed via the Internet and computers. Terms such as cyber crimes, computer crimes, internet crimes, information technology crimes, and high technology crimes have been used (Goodman and Brenner 2002). Although the terms "cyber crime", "computer crimes", "information crimes" and "virtual crimes" are preferred in general use, these expressions may vary depending on the computer, internet network, and technological devices used in the commission of the crime. "Computer crimes" was a concept used in the periods before the invention of the Internet. Today's accepted and widely used term is "cybercrime" (Moitra 2005).

Although there is no entirely accepted definition of cybercrime, different definitions have been made. Crimes committed against computers, depending on the orientation of a group, are considered cybercrime (Marsh and Melville 2009). According to another group, any crime committed via the Internet or computer-related is called cybercrime (Wall 2024). Cybercrime is a crime that targets the user and data security of another information system by using the information system (R. Ch and Al-Ahmari 2020). Cybercrime is crimes such as illegally entering information systems without permission, seizing data, deleting, changing, and blocking access to the system (IBM 2024). Cybercrime is any criminal activity that targets or uses computers, computer networks, or network-connected devices. Hackers who want to damage computer systems usually commit cybercrimes to gain profit or make money (W. A. Al-Khater and Khan 2020). In the most general sense, entering computer networks and all devices connected to these networks without permission and acting in a way that causes material and moral damage to individuals or institutions is a cybercrime (Wall 2024).

Manuscript received: 11 January 2025,
Revised: 24 January 2025,
Accepted: 24 January 2025.

[1]muraterdogan41@gmail.com (**Corresponding author**).
[2]ofarukakmese@hitit.edu.tr

For a cybercrime to occur, a crime triangle consisting of a victim, reason, and opportunity must be present (Lallie *et al.* 2021). The victim is the person attacked; the reason is the factor that pushes the criminal to commit the attack, and the chance to commit the crime is the opportunity. Cyber crimes committed today have become more complex. Sometimes, attacks are made against specific targets for reasons such as revenge, money, or espionage, while sometimes, attacks can be carried out with unclear motivations, which are opportunistic and aimless. The method of committing cyber crimes is changing day by day. For this reason, it is becoming increasingly difficult to intervene in cyber attacks and take security measures (K. Shaukat and Xu 2020).

With the increase in internet usage worldwide, the rate of cyber crimes has also increased (C. Lu and Chang 2007). Cyber crimes have caused significant financial losses to individuals, institutions, and countries. According to a report by the FBI in the USA, cyber crimes caused financial losses of 4.2 billion dollars worldwide in 2020, estimated to reach 6.9 billion dollars in 2021 (Cldy 2023). These results show us that more studies need to be done on cybercrime.

With the acceleration of scientific studies, large volumes of data have emerged. Making sense of these data and producing meaningful outputs for future research and studies is necessary. Bibliometric methods help researchers to examine previous studies in the literature before starting to examine a field of science and to discover the most influential studies in that field (Zupic and Čater 2015). Bibliometrics performs numerical analysis using different methods and techniques, such as data from various databases. The most influential authors, institutions, countries, keywords, and most cited sources, journals, and authors on a subject are found with bibliometric analysis. With bibliometric analysis, research and studies in the field of science are evaluated, the current situation is determined, and predictions for the future are made with these data (Şakar and Cerit 2013). Bibliometrics is used to measure the current status of institutions, journals, and authors and identify the most current topics, the most influential authors and documents, and collaborations in the field (Wang *et al.* 2018).

In their article titled "Trends in computer crime and cybercrime research during the period 1974-2006: A bibliometric approach", C. Lu and Chang (2007) conducted a bibliometric analysis of 292 publications related to cybercrime from 1974 to 2006. The study includes the review of publications in the form of articles, editorial materials, reviews, and meeting abstracts without any language or document type limitation. The study also states that computer crimes increased with the increase in internet users and internet applications from 1991 to 2000, after the development of web browsers. It was also announced that research on cybercrime is needed to reduce and prevent cybercrime activities.

Ho and Luong (2022) made a bibliometric analysis of the victimizations encountered after cybercrimes in their article titled " Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis". The research analyzed 387 articles bibliometrically from the Web of Science database on cyber crime victimization between 2010 and 2020. Keywords related to cybercrime victimization: "cyber bullying" (174 times), "cyber victimization" (90 times), "adolescent" (79 times), "bullying" (66 times), "victimization" (56 times), ' It was determined that 'cyber crime' (40 times) and 'cyber aggression' (37 times) were mentioned. The study aimed to identify global collaborations, research gaps, and existing gaps in cybercrime victimization research.

In their article titled "Research trends in cybercrime and cybersecurity: A review based on Web of Science core collection database", L. Wu and Lembke (2023) conducted a bibliometric review of research trends in cybercrime and cybersecurity between 1995 and 2021. The research examined 3635 publications containing the keywords "cyber crime" and/or "cyber security" using the bibliometric method. The study aims to comprehensively reveal the scientific landscape of the field by examining publications on cybercrime and cyber security and presenting multiple perspectives. The research shows that studies in Cyber Crime and Cyber Security have increased rapidly in recent years and that this field is a developing field of research.

In their article titled "The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index", Subektiningsih and Hariyadi (2022) conducted a bibliometric analysis of research on the field of Cyber Crime and/or Computer Forensics in Indonesia between 2010 and 2021. In the research, 281 articles were accessed from the Scopus database with the keywords "Cyber Crime" or "forensic investigation" or "digital forensics" or "computer crimes" and "Indonesia". 281 articles related to this field in Indonesia were analyzed with bibliometric analysis tools. The study identified universities and academicians working in cybercrime and digital forensics in Indonesia. The research is thought to positively impact law enforcement agencies solving cybercrime investigations by making scientific publications of computer forensic experts. In their article titled "Cybersecurity Trend Analysis Using Web of Science: A Bibliometric Analysis", Shukla and Gochhait (2020) analyzed cybersecurity-related articles between 1998 and 2020 using bibliometric methods. For the research, more than 2000 thousand studies were analyzed bibliometrically with VOSviewer and Excel programs using the keywords "Cyber Security" or "cyber security" from the Web Of Science database. The literature of every study published in cybersecurity was analyzed.

In their article titled "Cyberbullying research — Alignment to sustainable development and impact of COVID-19", K. Achuthan and Raman (2023) aimed to provide a bibliometric perspective on cyberbullying research between 2010 and 2021, including post-COVID-19. The research analyzed 7045 publications written about Cyberbullying between 2010 and 2021 using bibliometric methods. In the research, it was determined which countries contributed to publications on Cyberbullying and how much. The study sought answers to questions such as whether COVID-19 impacts Cyberbullying and whether Cyberbullying research is compatible with sustainable development goals. The research includes examining where we come from and where we will go in the future regarding Cyberbullying through bibliometric analysis.

M. M. Alashqar and Aziz (2021), in their article "Examining the trend of research on chemometric analysis: a bibliometric review", conducted a bibliometric analysis to evaluate cyber crime research. The study analyzed 377 publications from the Spocus database with bibliometric methods in searches related to "cyber crime" from 1998 to 2022. The study found that the most effective countries in cybercrime are the USA, Australia, and the UK. It was observed that the English language was used in 98% of 377 publications. It has been emphasized that the increase in the addiction level of internet use of businesses, communities, and individuals has led to an increase in cyber crimes. These studies are thought to contribute to academics, students, and experts' understanding of the development of cyber security as a research field.

This study presents the bibliometric analysis of 2566 studies indexed in the Web of Science database between 2000 and 2023. The spread of the internet and computer technologies worldwide since 2000 caused us to choose this year as the starting point. Our study

aims to reveal the scientific landscape of the cyber crime field. This study, which covers the best authors, countries, keyword features, collaborations, and the review of the most important articles, offers the opportunity to track the studies on cybercrime historically using appropriate bibliometric analysis techniques. This study aims to evaluate the published studies on cybercrime numerically, make sense of the data related to cybercrimes, reveal how the subject has developed over time, and create a scientific map of the field.

MATERIAL AND METHODS

Bibliometric analyses allow a numerical analysis of the effectiveness of publications in a certain field. Bibliometric techniques offer us an examination method with data sets to examine the relationship between scientific studies and evaluate research activities (Borgman and Furner 2001). WoS is both a research tool that supports comprehensive scientific examination of studies from various disciplines and the world's leading scientific citation search platform that allows working with large-scale data (K. Li and Yan 2018). WoS includes more than 21 thousand journals and over 200 thousand conference proceedings from more than 250 disciplines. For this reason, the WoS database was preferred to collect the data set. WoS is a website that regularly scans many journals, publications, and conferences worldwide. It also gives researchers access to numerous databases for more comprehensive bibliometric studies. Researchers dealing with bibliometric analysis use WoS as a data source in their research (Soydal and Al 2014).

All publications indexed in WoS regarding Cyber Crimes between 2000 and 2023 (accessed on 15.01.2024) were analyzed with bibliometric methods. The keywords "Cyber Crimes" or "Internet Crimes" or "Computer Crimes" were used for the search. Documents were searched by filtering by article title, abstract, and keywords. WoS codes used in our search: ("Cyber Crimes" or "Internet Crimes" or "Computer Crimes") and (EXCLUDING PUBYEAR,1980) and(EXCLUDING PUBYEAR,1999) and (EXCLUDING PUBYEAR,2024). Using this search method, all publications published in the WoS database between 2000 and 2023, containing "Cyber Crimes" or "Internet Crimes" or "Computer Crimes" in their title, abstract and keywords, were found. The bibliometric mapping and visualization processes used Microsoft Excel and Bibliometrix software.

BIBLIOMETRIC ANALYSIS OF PUBLICATIONS RELATED TO CYBER CRIMES

Literature Research Review

There are 2566 studies published in different genres from 2000 to 2023. Articles (1317, 52%), proceedings (925, 36%), book chapters (130, 5%), review articles (58, 2%), book reviews (28, 1%), and others (108, 4%) were found as. As shown in Figure 1, articles on Cyber Crime are in different disciplines; "Computer Science" (2123, 46%), "Engineering" (731, 16%), "Criminology" (462, 10%), "Telecommunications" (446, 10%), "Law" (178, 4%), "Multidisciplinary et al" (625, 14%). Since the studies can fall into more than one discipline category, the total number of studies is more than 2566.

Development of Publications

Figure 2 shows the total number of publications by year. Despite some fluctuations, there is a general increase in publications from 2000 to 2023. The fact that studies on cybercrime started to develop after 2000 and are still developing shows us that the field

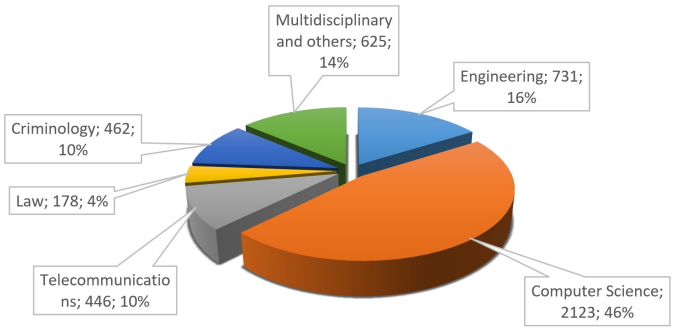


Figure 1 The Distribution of Subject Areas

is widespread. The fact that the number of studies has increased significantly between 2019 and 2023 reveals that studies on cyber crimes are very current. Although the number of publications has decreased in 2023, cyber crimes continue to affect our daily lives and all sectors.

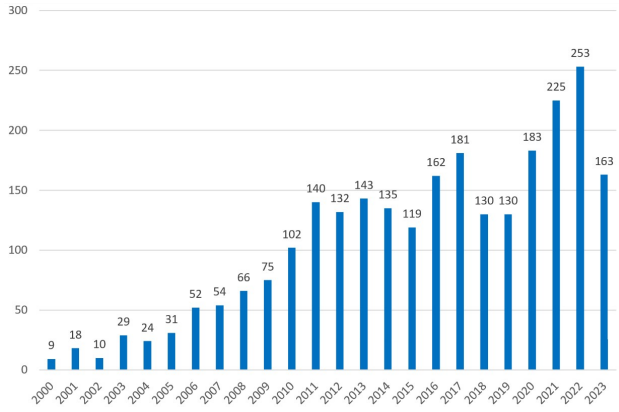


Figure 2 Annual Number of Publications by Year

Active Authors

5559 authors made a total of 2556 publications. Of these, 2829 authors' articles and 2032 authors' conference papers were published. Table 1 shows the 25 most influential authors with the highest h index on the topics "Cyber Crimes", "Computer Crimes" and "Internet Crimes". The top five authors with the highest h-index in the fields of "Cyber Crimes", "Computer Crimes" and "Internet Crimes" are Higgins G., Holt T., Liu Z., Choo K., L. J. There are indicators such as the number of publications, citations, h-Index, G-Index, and M-Index that measure the individual performance of authors. Having a large number of publications by an author is an important criterion that shows the performance of that researcher. However, the number of publications alone does not indicate the author's effectiveness. The number of citations received by authors in their studies is another performance indicator that shows the effectiveness of researchers. However, just because a study receives many citations does not indicate that it is important and effective. Moreover, just because a study has never been cited does not mean it is unimportant and inefficient (Kaleci 2023). H-index is an index used to measure the productivity and performance of researchers (S. Firat and Kurutkan 2023). In calculating the H-index, the number of citations and publications received by the author in other publications are used.

Table 1 The top 25 most influential authors

No	Author	h-index	g-index	m-index	TC	NP	PY_Start
1	HIGGINS GE	9	15	0.429	454	15	2004
2	HOLT TJ	8	12	0.500	728	12	2009
3	LIU Z	7	10	0.500	110	14	2011
4	CHOO KKR	6	12	0.429	515	12	2011
5	LI J	6	10	0.750	104	11	2017
6	LI Y	6	13	0.353	214	13	2008
7	MARCUM CD	6	10	0.429	189	10	2011
8	ROGERS MK	6	10	0.286	240	10	2004
9	WANG J	6	11	0.429	138	12	2011
10	WU J	6	9	1.200	95	9	2020
11	BOURKE ML	5	5	0.313	231	5	2009
12	BREITINGER F	5	8	0.417	105	8	2013
13	CHEN Y	5	9	0.357	126	9	2011
14	JAISHANKAR K	5	10	0.278	119	21	2007
15	LI Z	5	9	0.278	91	10	2007
16	SEIGFRIED-SPELLAR KC	5	10	0.357	103	10	2011
17	WANG L	5	7	1.000	62	7	2020
18	ZHANG H	5	9	0.556	99	9	2016
19	ALAZAB M	4	4	0.364	159	4	2014
20	ASRARI A	4	5	1.000	28	5	2021
21	BAGGILI I	4	12	0.250	161	12	2009
22	BOSSLER AM	4	5	0.250	576	5	2009
23	CARTHY J	4	4	0.308	127	4	2012
24	CASEY E	4	6	0.267	71	6	2010
25	CRAUN SW	4	4	0.364	90	4	2014

TC: Total Citation, NP: Number of Publications, PY_Start: Publication Year Start

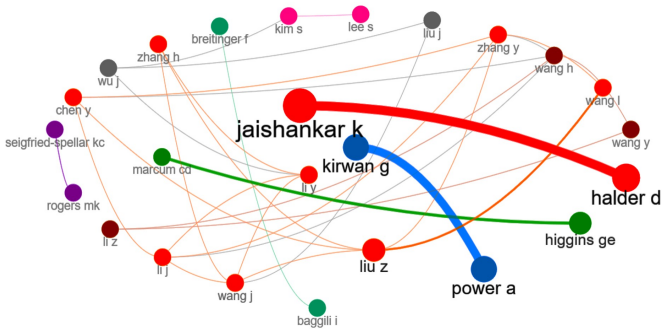


Figure 3 Authors Collaboration Network

Figure 3 shows the collaboration network among authors in publications related to cybercrime. The larger the circle, the greater the collaboration. Clusters are separated by colors. The power of collaboration between authors is expressed in the thickness of the lines.

Active Institutions

Figure 4 shows the graph of universities' publication production on cybercrime between 2000 and 2023. Figure 5 shows the co-operation network map of universities in the field. The greater the cooperation between universities, the greater the number and thickness of the lines. The more work there is, the larger the flat size.

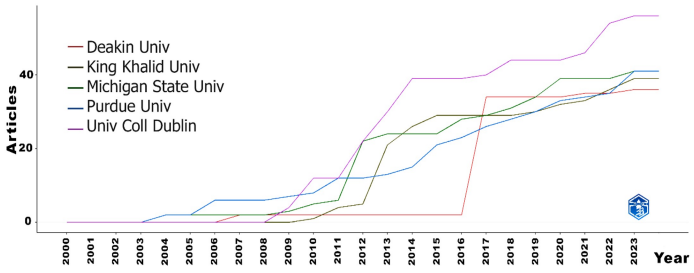


Figure 4 Number of Publications by Institutions in the Period 2000-2023

Table 2 shows the top 25 universities across countries that publish the most on "Cyber Crimes", "Computer Crimes" and "Internet Crimes". The universities with the most publications on cybercrime were College Dublin University, with 56 publications; Michigan State University, with 41 publications; Purdue University, with 41 publications; King Khalid University, with 36 publications; and Deakin University, with 31 publications.

Table 2 Top 25 Universities by Total Publications

No	University Name	Total Publications
1	UNIV COLL DUBLIN	56
2	MICHIGAN STATE UNIV	41
3	PURDUE UNIV	41
4	KING KHALID UNIV	36
5	DEAKIN UNIV	31
6	KOREA UNIV	31
7	DUN LAOGHAIRE INST ART DESIGN AND TECHNOL	28
8	KING SAUD UNIV	28
9	UNIV ALABAMA	28
10	UNIV LOUISVILLE	28
11	UNIV PRETORIA	27
12	KING ABDULAZIZ UNIV	26
13	TSINGHUA UNIV	25
14	UNIV WISCONSIN	25
15	CENT POLICE UNIV	24
16	MANONMANIAM SUNDARANAR UNIV	24
17	UNIV NEW HAMPSHIRE	24
18	UNIV S FLORIDA	24
19	UNIV TEXAS SAN ANTONIO	24
20	CTR CYBER VICTIM COUNSELLING	23
21	UNIV NEW HAVEN	23
22	A (CORRESPONDING AUTHOR)	22
23	DEPT COMP SCI	22
24	UNIV NEW SOUTH WALES	22
25	NATL INST TECHNOL	21

Figure 5 shows the collaboration network of the top 25 institutions. The larger the circle, the greater the collaboration. Clusters are separated by colors. The power of interinstitutional collaboration is expressed in the thickness of the lines.

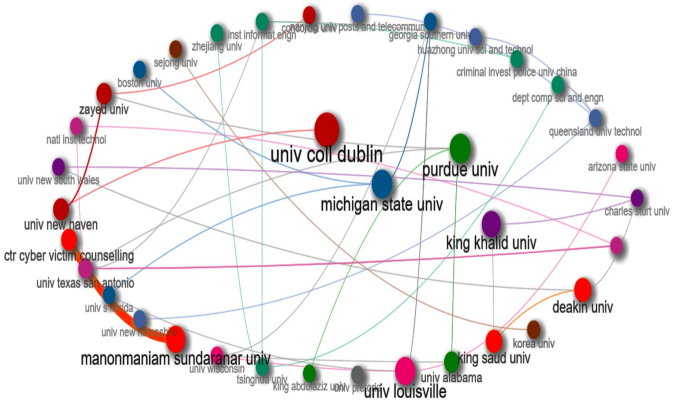


Figure 5 Inter-institutional Collaboration Network

Active Journals

In total, 1510 articles were published in 1243 journals. Table 3 shows the top 25 most influential journals with the highest *h_index* value on the subjects of "Cyber Crimes", "Computer Crimes", and "Internet Crimes." According to the table, *IEEE Access*, *International Journal of Cyber Criminology*, *Digital Investigation*, *Computers & Security*, and *IEEE Internet of Things Journal* are the most productive journals, respectively. Approximately 21% of the 1510 articles were published in these 25 journals.

The first five most influential journals are journals that support open access. Open communication journals are journals where scientific content can be accessed freely over the Internet. These journals aim to provide open and free access to scientific knowledge, often by eliminating financial barriers such as subscription, licensing fees, or pay-per-view. Enabling researchers to access scientific information more easily has made journals such as *IEEE Access*, *International Journal of Cyber Criminology*, *Digital Investigation*, *Computers & Security*, and *IEEE Internet of Things Journal* the most effective journals and resources.

Figure 6 shows data on the co-citation network among the 25 most influential journals. The size of the circle shows us that there are many of citations from that circle. Clusters are separated by colors. The greater the cooperation between journals, the greater the line thickness. Figure 7 shows the article production amounts of the six journals with the most articles by year. The remarkable result here is the IEEE Access journal started publishing in this field in 2016 and was a journal that published a small number of publications before 2018. However, IEEE Access magazine has rapidly increased its publications on cybercrime since 2018. The International Journal of Cyber Criminologists started publishing on cyber crimes in 2007, and the journal steadily increased its publication production until 2023.

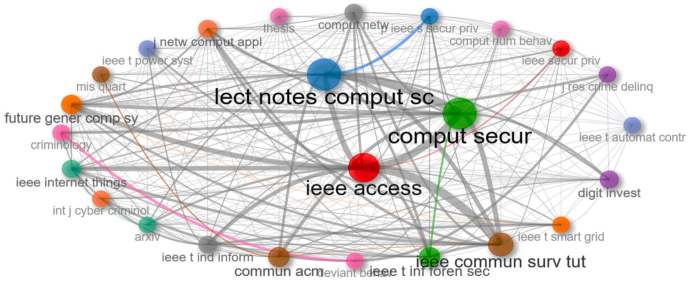


Figure 6 Sources Co-Citation Network

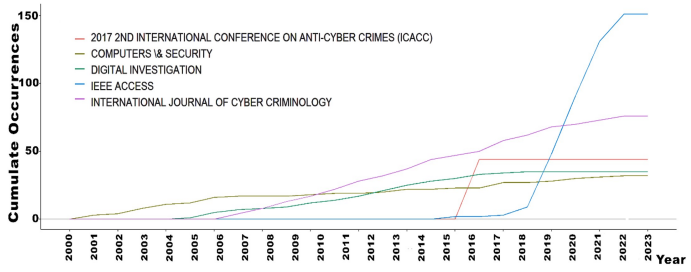


Figure 7 Top 6 Journals with the Most Articles

Distribution by Countries

Figure 8 shows the cooperation map between countries in articles on "Cyber Crimes", "Computer Crimes" and "Internet Crimes". The greater the cooperation between countries, the greater the number and thickness of the lines. Countries such as the USA (USA), China, India, and the UK (United Kingdom) are the most cooperative and leading countries in Cyber Crimes. Figure 9 shows the annual production amounts of publications on cybercrime by

Table 3 Top 25 Journals with h-index in Cybercrime Research

No	Journals	h-index	g-index	m-index	TC	NP	PY_Start
1	IEEE ACCESS	24	36	2.667	1920	151	2016
2	INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY	21	34	1.167	1293	76	2007
3	DIGITAL INVESTIGATION	17	23	0.85	602	35	2005
4	COMPUTERS & SECURITY	15	32	0.625	1330	32	2001
5	IEEE INTERNET OF THINGS JOURNAL	10	18	2	337	23	2020
6	IEEE SYSTEMS JOURNAL	10	16	2	268	21	2020
7	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	10	14	0.667	234	14	2010
8	IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT	10	19	1.667	378	20	2019
9	IEEE TRANSACTIONS ON SMART GRID	9	12	1.8	187	19	2020
10	2017 2ND INTERNATIONAL CONFERENCE ON ANTI-CYBER CRIMES	8	12	1	223	44	2017
11	CRIME LAW AND SOCIAL CHANGE	8	8	0.4	185	8	2005
12	IEEE TRANSACTIONS ON CYBERNETICS	8	10	1.6	285	10	2020
13	IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	8	17	0.727	314	24	2014
14	IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS	8	17	1.6	306	17	2020
15	IEEE COMMUNICATIONS SURVEYS AND TUTORIALS	7	8	0.7	409	8	2015
16	IEEE SECURITY & PRIVACY	7	11	0.467	198	11	2010
17	IEEE NETWORK	6	8	0.429	181	8	2011
18	IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT	6	14	0.286	214	15	2004
19	IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS	6	6	2	200	6	2022
20	POLICING-AN INTERNATIONAL JOURNAL OF POLICE STRATEGIES	6	7	0.286	193	7	2004
21	VICTIMS & OFFENDERS	6	6	0.375	105	6	2009
22	COMPUTER STANDARDS & INTERFACES	5	7	0.278	63	7	2007
23	CYBER CRIMINOLOGY: EXPLORING INTERNET CRIMES	5	9	0.357	101	25	2011
24	DIGITAL FORENSICS AND CYBER CRIME	5	9	0.333	89	16	2010
25	DIGITAL FORENSICS AND CYBER CRIME, ICDF2C 2012	5	9	0.417	98	20	2013

TC: Total Citation, NP: Number of Publications, PY_Start: Publication Year Start

country. Figure 10 shows the top 25 countries that publish the most on cybercrime. The USA, China, India, England, and Australia are the five countries with the most broadcasts. Figure 11 shows the cooperation network between countries in studies on cyber. The greater the cooperation, the greater the line thickness between countries. The more work there is, the larger the flat size. Table 4 shows the total number of citations received by countries. The USA, the UK, China, Australia, and India are the countries most cited in studies on cybercrime.

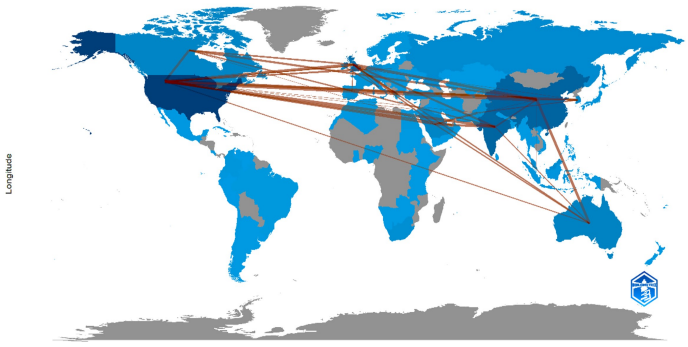


Figure 8 Countries Cooperation Map

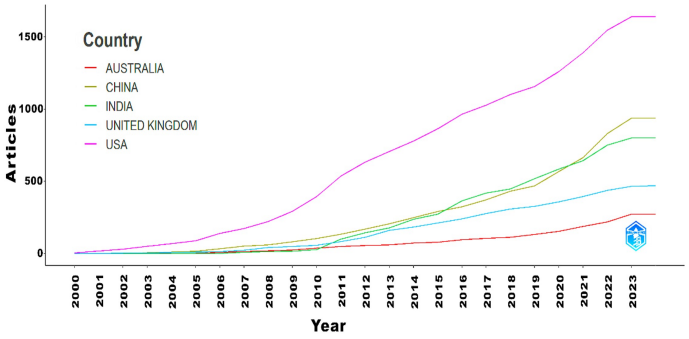


Figure 9 Production of Countries Over Time

Information About The Most Cited Journals, Publications, and Authors

Within the scope of the research on cyber crimes, the most cited journals, publications, and authors among 2566 studies were examined. Table 5 shows the first 25 publications according to the number of citations. The Stuxnet and the Future of Cyber War study is the most cited publication. The top 25 most cited journals are given in Table 6. The most cited journal is IEEE Access. The top 25 most cited authors are given in Table 7. The most cited author

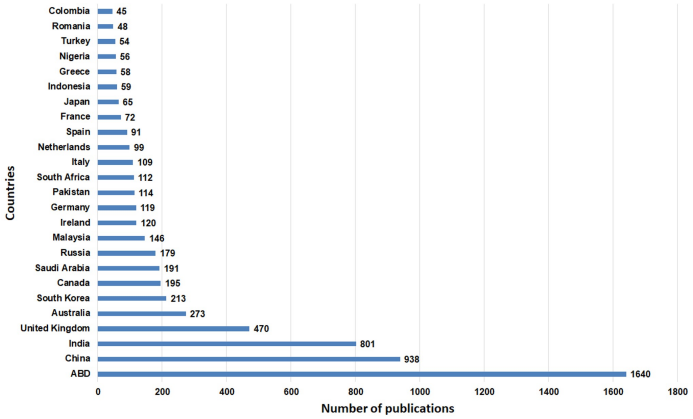


Figure 10 Bar Chart Showing the World's 25 Most Productive Countries

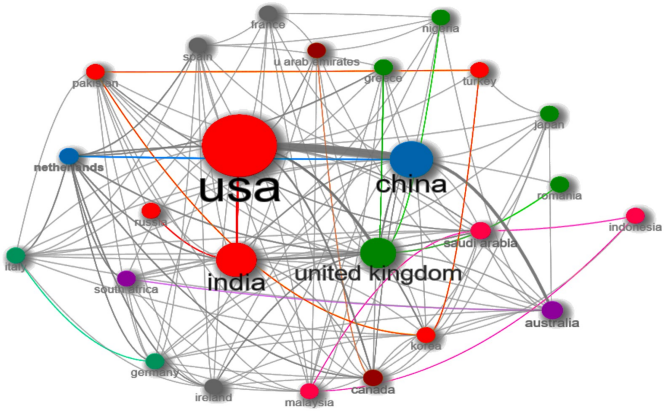


Figure 11 International Cooperation Network Map of Countries on Cybercrime

Table 4 Top 10 Countries by Total Citations in Cybercrime Research

No	Countries	Total Citation	Average Article Quotes
1	USA	8378	15.70
2	UNITED KINGDOM	2267	13.70
3	CHINA	2206	7.80
4	AUSTRALIA	1513	18.70
5	INDIA	1145	4.10
6	CANADA	718	11.60
7	SAUDI ARABIA	430	7.50
8	MALAYSIA	399	8.00
9	NETHERLANDS	384	12.00
10	SPAIN	373	10.70

is Higginsge, with a total of 93 citations. Writer Willison R follows Higgins Ge with 31 citations and writer Holt Tj with 30 citations.

Keyword Analysis

The change in keywords over time is an important indicator for understanding and monitoring developments in a research field. These changes may reflect changes in a topic's popularity, importance, and focus. It is also important to keep abreast of new terms and concepts that arise due to technological advances, societal changes, or other factors. In addition, keywords reflect the authors' work in the best way. These keywords are important elements that summarize the field and highlight research trends. Figure 12 shows the network visualization map analysis of the 25 most frequently used keywords across studies. The size of the circles increases depending on the frequency of use of keywords. The line thickness between keywords increases as the words are used together frequently, which shows the strength of the relationship between them. Clusters are separated by different colors. Computer crime, cybercrime, security, Internet, digital forensics, and machine learning were publications' most frequently used keywords. Table 8 shows the top 25 keywords most used in cybercrime-related publications. In the studies, the word computer was used 601 times, the word cybercrime 410 times, the word security 253 times, the word Internet 128 times, and the word digital forensics 127 times. Figure 12 shows the top 25 most used word clouds. Font sizes are large compared to the word repetition used.

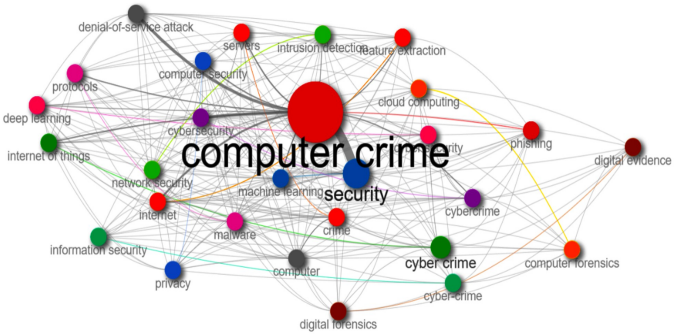


Figure 12 Keyword Analysis

Figure 13 Top 25 Most Used Word Clouds

Thematic Evolution

Keywords are the words that authors think best reflect their work. Therefore, it is very important to see which terms have been used in studies conducted on cybercrime to date to understand the current literature and future trends. This helps you evaluate the popularity and importance of certain terms. For this reason, keywords in the literature were determined, and the frequency of use and change of these words over time were analyzed. Figure 14 shows the analysis of the change and transformation of the most frequently used keywords in studies over the years. In this analysis, 2010 was chosen as the cutting year. Examining Figure 14 reveals that between 2000 and 2010, many terms, such as hacker, security, privacy, computer crime, internet crime, technology, etc., have evolved into cybercrime and computer crime in subsequent years.

Table 5 Top 25 Papers in Cybercrime Research by Total Citation

No	Paper	Total Citation	Annual Citation	Normalized Citation
1	Stuxnet and the Future of Cyber War	460	32.86	43.45
2	Beyond Deterrence: An Expanded View Of Employee Computer Abuse	294	24.50	27.25
3	Password Cracking Using Probabilistic Context-Free Grammars	253	15.81	10.41
4	Examining The Applicability Of Lifestyle-Routine Activities Theory For Cybercrime Victimization	235	14.69	9.67
5	The Cyber Threat Landscape: Challenges And Future Research Directions	231	16.50	21.82
6	Botnet Detection Based On Traffic Behavior Analysis And Flow İntervals	185	15.42	17.15
7	On-Line Activities, Guardianship, And Malware Infection: An Examination Of Routine Activities Theory	169	10.56	6.96
8	Cyber Security İn The Age Of Covid-19: A Timeline And Analysis Of Cyber-Crime And Cyber-Attacks During The Pandemic	161	40.25	16.61
9	A Survey On Technical Threat İntelligence İn The Age Of Sophisticated Cyber Attacks	161	23.00	23.00
10	Secure Cooperative Event-Triggered Control Of Linear Multiagent Systems Under Dos Attacks	160	32.00	11.34
11	A Survey Of Botnet And Botnet Detection	159	9.94	6.55
12	Low Self-Control, Deviant Peer Associations, And Juvenile Cyberdeviance	144	11.08	15.15
13	The 'Butner Study' Redux: A Report Of The Incidence Of Hands-On Child Victimization By Child Pornography Offenders	141	8.81	5.80
14	Insiders' Protection Of Organizational Information Assets: Development Of A Systematics-Based Taxonomy And Theory Of Diversity For Protection-Motivated Behaviors	140	11.67	12.97
15	Hidden Wholesale: The Drug Diffusing Capacity Of Online Drug Cryptomarkets	135	15.00	14.63
16	Botnet In Ddos Attacks: Trends And Challenges	133	13.30	13.76
17	Can Low Self-Control Help With The Understanding Of The Software Piracy Problem?	130	6.50	9.10
18	The Law Of Cyber-Attack	125	9.62	13.15
19	Exploring The Attack Surface Of Blockchain: A Comprehensive Survey	120	24.00	8.51
20	Choice And Chance: A Conceptual Model Of Paths To Information Security Compromise	118	7.38	4.86
21	A Survey On Machine Learning Techniques For Cyber Security In The Last Decade	117	23.40	8.29
22	Predicting Online Harassment Victimization Among A Juvenile Population	117	9.00	12.31
23	Sexual Violence In The Digital Age: The Scope And Limits Of Criminal Law	114	12.67	12.35
24	Lucid: A Practical, Lightweight Deep Learning Solution For Ddos Attack Detection	114	22.80	8.08
25	Estimating The Contextual Risk Of Data Breach: An Empirical Approach	113	11.30	11.69

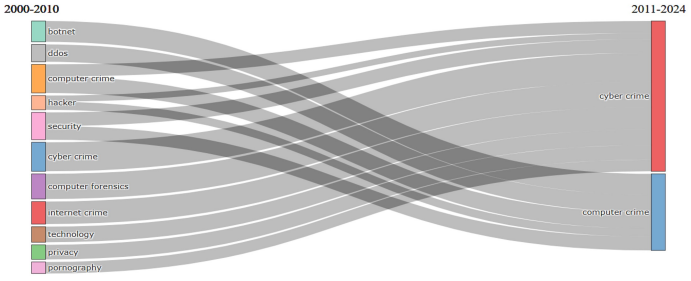


Figure 14 Thematic Development According to Author's Keywords

Trending topics

Based on the analysis of keywords, it was found which topics were more popular and which areas were researched between 2011 and 2023. Figure 15 shows which words and topics were used in publications related to cybercrime during specific years. It is possible to see that these topics evolved according to developments in the literature and new trends in the field of cybercrime. When we examine Figure 14, we see that in 2019, the most frequently used words were cybercrime, crime, and computer. In 2020, security, malware, and botnet were most commonly used. In 2021, the words computer crime, cybersecurity, and machine learning were prominent. In 2022, deep learning, Internet of Things (IoT), and denial-of-service attacks were the most frequently used words. The size of the circles increases with the frequency of word usage. The lines indicate the years during which the words were used. Based on this information, the most current and popular subtopics in cybercrime are deep learning, the Internet of Things, denial-of-service attacks, machine learning, and security. Therefore, researchers in the field of cybercrime should also pay attention to these topics.

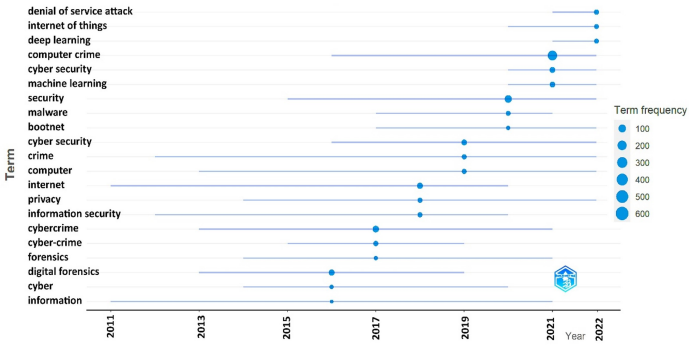


Figure 15 Popular topics used in cybercrime studies over time

Table 6 Top 25 Journals by Total Citations in Cybercrime Research

No	Journals	Total Citation
1	IEEE ACCESS	1920
2	COMPUTERS & SECURITY	1330
3	INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY	1293
4	DIGITAL INVESTIGATION	602
5	IEEE INTERNET OF THINGS JOURNAL	337
6	IEEE SYSTEMS JOURNAL	268
7	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	234
8	IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT	378
9	IEEE TRANSACTIONS ON SMART GRID	187
10	2017 2ND INTERNATIONAL CONFERENCE ON ANTI-CYBER CRIMES (ICACC)	223
11	CRIME LAW AND SOCIAL CHANGE	185
12	IEEE TRANSACTIONS ON CYBERNETICS	285
13	IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	314
14	IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS	306
15	IEEE COMMUNICATIONS SURVEYS AND TUTORIALS	409
16	IEEE SECURITY & PRIVACY	198
17	IEEE NETWORK	181
18	IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT	214
19	IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS	200
20	POLICING-AN INTERNATIONAL JOURNAL OF POLICE STRATEGIES	193
21	VICTIMS & OFFENDERS	105
22	COMPUTER STANDARDS & INTERFACES	63
23	CYBER CRIMINOLOGY: EXPLORING INTERNET CRIMES AND CRIMINAL BEHAVIOR	101
24	DIGITAL FORENSICS AND CYBER CRIME	89
25	DIGITAL FORENSICS AND CYBER CRIME, ICDF2C 2012	98

Table 7 Top 25 Authors by Total Citations in Cybercrime Research

No	Authors	Total Citation
1	HIGGINS GE	93
2	WILLISON R	31
3	HOLT TJ	30
4	MARCUM CD	28
5	MAKIN DA	23
6	BOSSLER AM	20
7	CHOO KKR	19
8	JAISHANKAR K	18
9	BACKHOUSE J	16
10	GRABOSKY P	15
11	ROGERS MK	15
12	SIPONEN M	15
13	ALAZAB M	14
14	BROADHURST R	14
15	CHON S	14
16	DONNER CM	14
17	HEARTFIELD R	14
18	JENNINGS WG	14
19	LOUKAS G	14
20	EPIPHANIOU G	13
21	EROLA A	13
22	LALLIE HS	13
23	MAPLE X	13
24	NURSE JRC	13
25	SHEPHERD LA	13

Table 8 Top Keywords in Cybercrime Research by Frequency of Use

No	Keyword	Number of Uses
1	Computer Crime	601
2	Cyber crime	410
3	Security	253
4	Internet	128
5	Digital Forensics	127
6	Cyber security	121
7	Machine Learning	108
8	Cyber security	105
9	Denial of Service Attack	79
10	Cyber crime	77
11	Crime	71
12	Computer	70
13	Privacy	68
14	Information security	67
15	Malware	64
16	Deep Learning	62
17	Internet of Things	62
18	Computer Security	61
19	Intrusion Detection	58
20	Servers	56
21	Cloud computing	55
22	Digital Evidence	54
23	Computer Forensics	51
24	Feature Extraction	51
25	Phishing	49

DISCUSSION

The dependence of societies and individuals on computers and the Internet is increasing daily. With the widespread use of the Internet and computers in business, entertainment, and government, crimes have moved to the virtual environment, and cybercrime has become increasingly important. Today, the majority of businesses and individuals are exposed to cybercrime. This situation has caused academics to search for solutions and research how to deal with cybercrime. For this reason, it has been observed that the interest in the field of research on cybercrime has increased significantly in recent years, and the demand for scientific research on this subject has increased. Due to the lack of knowledge and increasing dangers in the field of cybercrime, the importance of research in this field is increasing. The rapid and consistent growth of publications on cybercrime over time shows that the subject is a growing and developing field of research.

Cyber crimes, which cause material and moral losses to individuals, institutions, and countries, are committed in multiple ways and for different reasons. Privacy is violated due to phishing, theft, and breach of personal data through phishing. Personal information is used to obtain material and moral benefits. Cybercrime, which is the deletion, corruption, and modification of data belonging to individuals and institutions, is committed by seizing information systems and computer networks. Again, bank and credit card information is obtained through phishing and spam e-mail methods, and this information is misused. With romantic fraud, financial benefits are obtained by exploiting people's well-intentioned feelings and thoughts. By infecting the system with malware and viruses, both information is seized, and a type of

cyber extortion is carried out by demanding ransom.

In our research, despite the fluctuations in the distribution of the number of publications related to cybercrime over the years 2000 to 2023, it is seen that the number of publications has generally increased. It was observed that the number of publications increased rapidly from 2019 to 2022, and the number of publications decreased slightly from 2013 to 2015 and from 2017 to 2018. It was observed that the number of publications remained the same from 2018 to 2019. When the production amounts of publications are examined by years, approximately 85% of the 2566 studies were published after 2010. It was observed that most publications in the field of cybercrime were published in 2022 (253 studies). It was found that the most common type of publication in the field was articles with 1317 studies. This was observed, followed by papers with 925 studies, book chapters with 130 studies, and review articles with 58 studies. When the WoS science network categories for studies on cybercrime were examined, it was found that most studies were in the computer science category, with 2123 studies. The computer science category was followed by engineering with 731 studies, criminology with 462 studies, and telecommunications with 446 studies.

Authors with the highest h_index on the subject: Higgins Ge, Holt Tj, Choo Kkr, Marcum Cd. Wang J. The journals with the highest h_index on the subject are *IEEE Access*, *International Journal of Cyber Criminologists*, *Digital Investigation*, *Computers & Security*, and *IEEE Internet of Things Journal*. The institutions with the highest h-index in this subject area are University College Dublin, Michigan State University, Purdue University, King Khalid University, and Deakin University. It is thought that the geographical locations of countries impact international cooperation. When the number of publications by country is evaluated, it is seen that the countries with high populations or great economic power, such as the USA, China, India, the United Kingdom, and Australia, publish the most studies on cybercrime.

The most cited article was published in *Survival* magazine, "Stuxnet and the Future of Cyber War," by authors Farwell and Rohozinski (2011). The study became the most cited article, with 460 citations. The next most cited article was published in *MIS Quarterly* magazine by authors Willison and Warkentin (2013), titled "Beyond Deterrence: An Expanded View Of Employee Computer Abuse". The article ranked second with a total of 294 citations. The next most cited article was published in the *IEEE Xplore* journal by authors M. Weir and Glodek (2009), titled "Password Cracking Using Probabilistic Context-Free Grammars". This study ranks third with a total of 253 citations.

When the words used in the articles are evaluated, computer crime, cybercrime, security, Internet, digital forensics, cyber security, and machine learning are the most frequently used keywords. The word *computer* was used 601 times, the word *cybercrime* 410 times, the word *security* 253 times, the word *Internet* 128 times, and the word *digital forensics* 127 times. One of the limitations of the current study is that it does not include data from bibliometric databases other than the WoS database. Again, the study is limited since the research and publications in the WoS database will be used from 2000 to 2023.

In this study, we determined the most important and current topics in the field of cybercrime based on a map consisting of author keywords. We hope this type of analysis will help scholars understand the changing scientific landscape of cybercrime research. Generally speaking, deep learning, the Internet of Things, denial of service attacks, machine learning, and cyber security issues have been among the popular topics in cybercrime in recent years. This study emphasizes that the scientific literature on cybercrime is growing and important. The research aims to guide researchers who want to gain information about future studies and trends on these issues. This study guides academics in planning and conducting their research on cybercrime. Our study contributes to understanding the trends and developments of scientific research on cybercrime. Our research focuses on identifying trends in the field of cybercrime and addressing gaps in this field. In this context, it is important to focuscontext, it is important to focus more on policies and studies to combat cybercrime and protect societies, companies, and states is important in this context.

CONCLUSION

This study provides a complete review of studies and publications on cybercrime between 2000 and 2023. The research used bibliometric analysis to examine global trends in cybercrime investigations over the last 23 years. Web of Science (WoS) database was used for bibliometric analysis. A total of 2566 publications, countries, institutions, journals, authors, and subject categories were analyzed to evaluate the effectiveness of studies on cybercrime. Although there has been a decrease from time to time in the number of publications produced over the years, there is a general increase. The country that publishes the most on the subject and where the most effective studies are carried out is the USA. Jaishankar Karuppannan is the most published author. The author who wrote the most influential works and has the highest h_index is George E. Higgins. The journal with the highest h_index and the most publications is *IEEE Access*. Again, the institution with the most publications and the highest h_index is College Dublin University. The most frequently used keyword in research is the term *computer crimes*. The most cited article was published in *Survival* magazine titled *"Stuxnet and the Future of Cyber Warfare"*. The best countries in cybercrime investigations are economically developed and populous countries. This analysis determined which countries, institutions, journals, authors, and subject categories are more effective in this field or contribute more to scientific studies. Considering the number of publications on the subject, the rapid increase in studies in the last two to three years reveals the need for more research on cybercrime. Dealing with cybercrime poses a big problem as the way cybercrime is committed changes day by day. Therefore, more research is needed to prevent and reduce cybercrime activities.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Borgman, A. and S. Furner, 2001 Scholarly communication and bibliometrics. Annual Review of Information Science and Technology **36**.

C. Lu, W. J. and W. Chang, 2007 Trends in computer crime and cybercrime research during the period 1974-2006: A bibliometric

approach. In *Intelligence and Security Informatics*, volume 4430 of *Lecture Notes in Computer Science*, pp. 244–250.
Cldy, 2023 Email spam statistics 2022 – find out more about spam emails. Accessed: Jan. 03, 2023.
Farwell, J. P. and R. Rohozinski, 2011 Stuxnet and the future of cyber war. Survival (London) **53**: 23–40.
Goodman, M. D. and S. W. Brenner, 2002 The emerging consensus on criminal conduct in cyberspace. International Journal of Law and Information Technology **10**: 139–223.
Ho, H. T. N. and H. T. Luong, 2022 Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. Springer International Publishing **2**.
IBM, 2024 What is a cyberattack? | ibm. Accessed: Jan. 28, 2024.
K. Achuthan, R. K. S. R., V. K. Nair and R. Raman, 2023 Cyberbullying research — alignment to sustainable development and impact of covid-19: Bibliometrics and science mapping analysis. Computers in Human Behavior **140**: 107566.
K. Li, J. R. and E. Yan, 2018 Web of science use in published research and review papers 1997–2017: a selective, dynamic, cross-domain, content-based analysis. Scientometrics **115**: 1–20.
K. Shaukat, V. V. I. A. H., S. Luo and M. Xu, 2020 A survey on machine learning techniques for cyber security in the last decade. IEEE Access **8**: 222310–222354.
Kaleci, F., 2023 Ekonomi alanındaki İnovasyon konulu uluslararası bilimsel yayınların bibliyometrik analizi .
Klimburg, A., 2018 *National cyber security framework manual*. Accessed: Apr. 12, 2023.
L. Wu, Q. P. and M. Lembke, 2023 Research trends in cybercrime and cybersecurity: A review based on web of science core collection database. International Journal of Cybersecurity Intelligence and Cybercrime **6**: 5–28.
Lallie, H. S., L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, *et al.*, 2021 Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security .
M. M. Alashqar, A. B. A. R. and A. S. B. A. Aziz, 2021 Examining the trend of research on chemometric analysis: a bibliometric review. Accessed: Apr. 12, 2023.
M. Weir, B. D. M., S. Aggarwal and B. Glodek, 2009 Password cracking using probabilistic context-free grammars. In *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 391–405.
Marsh, I. and G. Melville, 2009 *Crime, Justice and the Media*. Routledge.
Moitra, S. D., 2005 Developing policies for cybercrime: Some empirical issues. European Journal of Crime, Criminal Law and Criminal Justice **13**: 435–464.
Phillips, K., J. C. Davidson, R. R. Farr, C. Burkhardt, S. Caneppele, *et al.*, 2022 Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic Science **2**: 379–398.
R. Ch, M. H. A., T. R. Gadekallu and A. Al-Ahmari, 2020 Computational system to classify cyber crime offenses using machine learning. Sustainability **12**: 4087.
S. Firat, G. G. Y. K., B. O. Alramazanoğlu and M. N. Kurutkan, 2023 H-İndeksi ve akademik başarıyı Ölçme sorunu: Eksiklikler ve sınırlılıkları aşma Çabası. Mehmet Akif Ersoy Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi pp. 1742–1777.
Shukla, G. and S. Gochhait, 2020 Cyber security trend analysis using web of science: A bibliometric analysis. European Journal of Molecular and Clinical Medicine **7**: 6.
Soydal, and U. Al, 2014 Akademinin atıf dizinleri ile savaşı. Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi **31**: 23–42, Accessed: Apr. 12, 2023.
Subektiningsih, S. and D. Hariyadi, 2022 The role of digital forensic experts in cybercrime investigations in indonesia based on the scopus research index **4**: 1665–1670.
W. A. Al-Khater, A. A. A. A. S. S., S. Al-Maadeed and M. K. Khan, 2020 Comprehensive review of cybercrime detection techniques. IEEE Access **8**: 137293–137311.
Wall, D. S., 2024 *Cybercrime: The Transformation of Crime in the Information Age*. Accessed: Mar. 28, 2024.
Wang, W., S. Laengle, J. M. Merigó, D. Yu, E. Herrera-Viedma, *et al.*, 2018 A bibliometric analysis of the first twenty-five years of the international journal of uncertainty, fuzziness and knowledge-based systems. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **26**: 169–193.
Willison, R. and M. Warkentin, 2013 Beyond deterrence: An expanded view of employee computer abuse-web of science core collection. Accessed: Apr. 12, 2023.
Zupic, I. and T. Čater, 2015 Bibliometric methods in management and organization. Organizational Research Methods **18**: 429–472.
Şakar, G. D. and A. G. Cerit, 2013 Uluslararası alan İndekslerinde türkiye pazarlama yazını: Bibliyometrik analizler ve nitel bir araştırma. Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi **27**: 274201337–274201362, Accessed: Apr. 04, 2023.

How to cite this article: Akmeşe, Ö. F., and Erdoğan, M. Bibliometric Analysis of Studies on Cyber Crimes Between 2000-2023. *ADBA Computer Science*, 2(1), 19-29, 2025.