Revista Politécnica ISSN 1900-2351 (Impreso), ISSN 2256-5353 (En línea), Año 22, Número 43, páginas 62-82, Enero-Junio 2026

DOI: https://doi.org/10.33571/rpolitec.v22n43a5

ETHICAL HACKING BASED ON TRUST TESTS: A VISION ORIENTED TO CYBERSECURITY AND RISK MITIGATION

Paola A. Buitrago-Cadavid [1], John J. Castro-Maldonado [2], Bernardo Zapata-Baena[3], Robert D. Urda-Benitez[4]

[1] MSc in Modeling and Computational Science, Faculty of Engineering, National Open and Distance University, GIDESTEC Research Group, Medellin-Colombia. Email: paola.buitrago@unad.edu.co, https://orcid.org/0000-0001-8770-7794
[2] PhD en Educación, PhD en Ingeniería (C), Servicio Nacional de Aprendizaje SENA. Broward International University BIU. Email: jcastrom@sena.edu.co, johnjairo.castro@biu.us, https://orcid.org/0000-0002-3823-4297
[3] Ingeniero Electrónico, Servicio Nacional de Aprendizaje SENA. Email: bjzapata@sena.edu.co
[4] MSc in Industrial Automation and Control, Faculty of Engineering, Pascual Bravo University Institution, GICEI Research Group, Medellin-Colombia. Email: robert.urda@pascualbravo.edu.co, https://orcid.org/0000-0003-4921-5195

RESUMEN

In the context of growing cybersecurity threats across interconnected sectors, ethical hacking and penetration testing have become essential for protecting sensitive information and critical infrastructure. This systematic review analyzes recent literature on cybersecurity anomalies and identifies the most effective machine learning techniques used in critical domains such as healthcare, finance, and government. The findings reveal that anomalies AN05 and AN08 are among the most frequently reported threats, while techniques T01 and T18 are widely adopted for detecting attack patterns and strengthening cyber defense mechanisms. The review also examines the ethical and legal dimensions of ethical hacking, highlighting the need for sector-specific regulatory frameworks. Additionally, key research gaps are identified, including the lack of standardized trust-testing methodologies, limited transferability of machine learning models, and continued reliance on human expertise. Emerging artificial intelligence technologies offer promising opportunities to improve predictive capabilities, scalability, and cybersecurity resilience across diverse operational environments.

Palabras clave: Ethical Hacking, Penetration Testing, Security Testing, Vulnerability Assessment, Information Security, Cybersecurity, Cybert threats, Phishing

Recibido: 3 de noviembre de 2025. Aceptado: 13 de mayo de 2026
Received: November 3, 2026. Accepted: May 13, 2026

Cómo citar este artículo: A. Buitrago-Cadavid, J. Castro-Maldonado, B. Zapata-Baena, R. Urda-Benitez. "Ethical hacking based on trust tests: A vision oriented to cybersecurity and risk mitigation", Revista Politécnica, vol.22, no.43 pp.62-82, 2026. DOI:10.33571/rpolitec.v22n43a5

1. INTRODUCCIÓN

In the digital era, cybersecurity is essential for protecting critical infrastructures and sensitive data. As a result, ethical hacking activities and penetration tests are employed in sectors such as academia, economy, industry, automotive, and healthcare, which face increasing risks due to interconnectivity and the use of the Internet of Things (IoT). It is anticipated that by 2025, the IoT will have an economic impact of $11.1 trillion, with 75 billion connected devices [1]. The advancement of technologies such as artificial intelligence introduces new attack vectors, as phishing techniques have evolved and become more difficult to detect [2]; [3].

To counteract this, PhishStorm is proposed—an automated system that uses URL analysis to identify phishing sites with 96.50% accuracy [4]In the healthcare sector, blockchain frameworks are applied to protect sensitive data, and security architectures complying with standards such as HIPAA and FISMA are utilized [5]. Additionally, advanced techniques for phishing detection have been developed, enhancing security against emerging threats [6]. Furthermore, blockchain technology is being applied across various sectors to improve transparency and security. In the financial industry, it is utilized to optimize transaction execution, as demonstrated by the Interbank Spunta project. In education, it ensures the authenticity of academic certificates, and in healthcare, it securely manages medical data, allowing patients to control their records [7].

In the supply chain, a blockchain-based model has been developed that employs smart contracts on Ethereum to automate transactions, ensuring compliance without intermediaries and improving efficiency through decentralized storage using IPFS. This model includes a reputation system that fosters trust among participants [8]. However, the implementation of disruptive technologies such as the IoT and cloud computing in the manufacturing sector has generated new threats [8], especially in vulnerable sectors like finance and retail, where phishing remains a constant concern. To combat these threats, classification techniques such as Random Forest, Support Vector Machine, and Multilayer Perceptron, among others, are employed [9]. In the defense sector, blockchain and smart contracts are employed to ensure the integrity of transactions [10]. In the realm of IoT, vulnerabilities are detected through machine learning techniques [11].

Phishing is countered using deep learning and algorithms such as MLP [12]; [13], while in corporate networks, deep neural networks are utilized to predict threats. In Industry 4.0, cybersecurity is reinforced with digital twins and honeypots [14]. At the organizational level, insider threats are mitigated by analyzing cyber hygiene and assessing motivations before security is compromised [15]. In the realm of intelligent vehicles, intrusions and spoofing attacks are prevented using deep learning and hybrid techniques that safeguard vehicular networks [16]. Finally, authors such as [17]; [18] have identified advanced attacks in critical networks using anomaly-based approaches and multi-agent systems, highlighting the necessity for robust response techniques.

The objectives of this systematic review are: to analyze the current state of the literature on the incidence of anomalies in cybersecurity within critical sectors; to identify the most effective machine learning techniques used to enhance digital security; to explore the ethical and legal implications of ethical hacking and the most appropriate regulatory frameworks for each sector; and finally, to identify the main gaps in current research on ethical hacking and penetration testing, evaluating how the integration of emerging technologies, such as artificial intelligence, could address these gaps.

1.1 Research Questions

Research questions were established to analyze the literature on ethical hacking and penetration testing, 66 focusing on cybersecurity and risk mitigation in critical sectors. These questions guide the SLR and assess their impact on digital security.

Q1.) ¿What is the current state of the literature on the incidence of anomalies in cybersecurity and critical 69 sectors?
Q2.) ¿What are the most effective machine learning techniques used in cybersecurity in critical sectors, and what is their impact on improving digital security?
Q3.) ¿What are the ethical and legal implications of ethical hacking, and which regulatory frameworks are most suitable for each sector?
Q4.) ¿What are the main gaps in current research on ethical hacking and penetration testing, and how could the integration of emerging technologies, such as artificial intelligence, address these gaps?

2. MATERIALES Y METODO

The present systematic review has been conducted following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodological framework, aiming to ensure transparency and rigor in the selection and analysis of the literature. To achieve this, an exhaustive search was carried out in scientific databases such as IEEE Xplore and Scopus, selecting studies that addressed the topic of ethical hacking and penetration testing applied in cybersecurity using machine learning techniques.

The following selection criteria were established: From a total of 528 identified articles, 181 articles published between the years 2000 and 2024 were selected. These articles were chosen based on predefined inclusion and exclusion criteria, considering aspects such as the type of study, the target population, and the intervention. These criteria allowed for the delimitation of studies that provided an analysis of the current state regarding vulnerabilities, risks, and mitigation techniques in critical sectors, with a particular focus on cybersecurity. As areas of interest, the selected articles focused on evaluating vulnerabilities and risks in key sectors.

For example, in the healthcare sector, where technologies like the Internet of Things (IoT) face significant threats, risks associated with advanced persistent threats (APT) were analyzed, which compromise patient privacy [19]. In the industrial sector, the importance of protecting control systems to maintain operational continuity in critical infrastructures was highlighted [20]. In both sectors, techniques such as penetration testing and security audits were identified as essential for the detection of vulnerabilities and protection against threats [21]. Through the systematic literature review, ethical hacking is defined as the authorized practice of evaluating system security by simulating attacks to identify potential vulnerabilities. Similarly, penetration testing is established as procedures to simulate threats and analyze the response capacity of systems, while cybersecurity refers to the protection against digital attacks on critical infrastructures.

This approach allowed for the classification and analysis of machine learning techniques employed in risk mitigation specifically for each sector, underscoring the importance of standardized frameworks and robust cybersecurity practices to protect critical systems. In Phase 1, the PICO method [22], described in Table 1, was adopted, which facilitated the formulation of a specific bibliographic search strategy using the IEEE Xplore and SCOPUS databases. Additionally, the eligibility criteria for selecting relevant studies were detailed. Through Phase 2, two subsections were developed in which the research questions were formulated and the search techniques used in the repositories were defined, to ensure that the studies found were aligned with the research objective. Finally, in Phase 3, a synthesis of the collected data was performed, classifying the reviewed studies into different categories and carrying out the corresponding meta-analysis.

Tabla 1. Considerations of the PICO Method and Their Definitions

PICO Consideration	Definition
Population (P)	Studies focused on Ethical Hacking, Penetration Testing, Security Testing, Vulnerability Assessment, and Security Audits.
Intervention (I)	Implementation of Ethical Hacking and Penetration Testing Practices for System Security Assessment, Supported by Machine Learning Models for Threat Detection.
Comparison (C)	Comparison with Studies Addressing Trust-Based Services, Trust Management, Information Security, Cybersecurity, and Trust, Including Analysis of the Effectiveness of Machine Learning Models in These Contexts.
Results (O)	Focused on the Identification and Mitigation of Network Threats, Cyber Threats, Cyber Risk, as well as the Assessment of Wireless Network Security Audit, Phishing, and Ethical Phishing, Alongside the Effectiveness of Applied Machine Learning Models.

Phase 1: Establishment of the PICO Method and Eligibility Criteria

The PICO method [22] was utilized as a key strategy for bibliographic research, facilitating the identification of eligibility criteria for various works, studies, research, and articles. Techniques for structuring search strings were established, as shown in Table 2. To construct these strings, well-known and appropriate Boolean operators, such as ”AND” and ”OR,” were used, organizing the keywords according to the following search equation:

Tabla 2. Search Equation

Database	Search Equation
IEEE Xplore	(“Ethical Hacking” OR “Penetration Testing” OR “Vulnerability” “Assessment” OR “Security Audits”) AND (“Information Security” OR “Cybersecurity” OR “Trust”) OR (“Ethical Hacking” OR “Penetration Testing” OR “Vulnerability Assessment” OR “Security Audits”) AND (“Cyber Threats” OR “Phishing”) OR (“Information Security” OR “Cybersecurity” OR “Trust”) AND (“Cyber Threats” OR “Phishing”)
SCOPUS	TITLE-ABS-KEY(“Ethical Hacking” OR “Penetration Testing” OR “Vulnerability Assessment” OR ”Security Audits”) AND TITLE- ABS-KEY(”Information Security” OR ”Cybersecurity” OR ”Trust”) OR TITLE-ABS-KEY(”Ethical Hacking” OR ”Penetration Testing” OR ”Vulnerability Assessment” OR ”Security Audits”) AND TITLE-ABS-KEY(”Cyber Threats” OR ”Phishing”) OR TITLE-ABS- KEY(”Information Security” OR ”Cybersecurity” OR ”Trust”) AND TITLE-ABS-KEY(”Cyber Threats” OR ”Phishing”)

For the collection of scientific articles, the search criteria detailed in Table 3 were used. The following are the different filters applied to each criterion for information gathering:

a) Criterion 1: A total of 4697 primary analyses were compiled, using the first four inclusion and exclusion criteria as shown in Table 3. The search range covered the period from 2000 to 2024, with English as the primary language of publication, and included studies such as conferences, articles, books, book chapters, magazines, and early access articles.

b) Criterion 2: Only scientific articles were considered, resulting in a total of 528 studies. A total of 448 articles were filtered from the IEEE Xplore database and 80 articles from the SCOPUS database, and the metadata for each was subsequently downloaded.

c) Criterion 3: In the third filter, a systematic literature review (SLR) was conducted on each metadata using ASReview software, identifying 161 relevant articles from the IEEE Xplore metadata and 20 relevant articles from the SCOPUS metadata.

Tabla 3. Article Typology and Criteria Used

Database	Article Type	Criterion 1	Criterion 2	Criterion 3
IEEE Xplore	Conferences, Journals, Books, Magazines, Early Access Articles	4,697	448	161
SCOPUS	Conference paper, Article, Conference review, Book chapter, Book, Short survey, Review, Editorial	263	80	20

Phase 2: Search Criteria Used

Table 4 presents the terms used in the analysis along with their equivalents, which were employed to expand the search results and ensure broader coverage of the relevant literature.

Tabla 4. Terms Used in the Search

Terms	Equivalent Terms
Ethical Hacking	White Hat Hacking, Penetration Testing
Penetration Testing	Pentesting, Security Pen Testing
Vulnerability Assessment	Risk Assessment, Weakness Evaluation
Cybersecurity	Cyber Protection, IT Security
Information Security	Information Security, Data Protection
Phishing	Email Scams, Spoofing
Cyber Threats	Cyber Attacks, Digital Threats
Security Audits	Compliance Audits, Security Evaluation

To select the primary studies, inclusion criteria were applied based on temporal and geographic characteristics for the study population; exclusion criteria involved discarding studies outside the established time range, gray literature, and studies in languages other than English, as shown in Table 5.

Tabla 5. Inclusion and Exclusion Criteria

Mapping Type	Inclusion	Exclusion
Systematic Mapping	Articles in digital format, online, indexed, and published in IEEE Xplore and SCOPUS during the period from 2000 to 2024. Publication language: English. Only scientific articles.	Studies published before 2000. Studies published in languages other than English. Non-scientific articles, such as reviews, editorials, commentaries, and books.
Systematic Literature Review	Articles containing keywords in the title and abstract: Ethical Hacking, Penetration Testing, Vulnerability Assessment, Cybersecurity, Information Security, Phishing, Cyber Threats, Security Audits. Cybersecurity studies related to the mentioned keywords. Studies addressing Red Teaming techniques and security audits in wireless networks.	Articles that do not contain these keywords in the title or abstract. Studies not directly related to cybersecurity and the specified keywords. Studies that do not develop Red Teaming, pentesting, or ethical hacking activities relatedto cybersecurity.

Phase 3: Data Synthesis and Classification of Reviewed Studies

Data Synthesis and Classification of Reviewed Studies Information was extracted from the articles selected in Phase 1, then each study conducted in the literature on cybersecurity anomalies, affected sectors, and finally, implemented machine learning techniques were structured and synthesized.

3. RESULTS AND DISCUSSION

3.1 Q1. What is the current state of the literature on the incidence of cybersecurity nomalies in critical sectors?

In the reviewed literature, various cybersecurity anomalies have been identified, arising from deliberate attempts at unauthorized system access aimed at disrupting functionality or extracting sensitive information through the introduction of malicious software. Such actions can seriously compromise the security of the systems involved. The main detected anomalies, represented as (AN #), where corresponds to the specific anomaly number, are detailed in Table 6.

Regarding the anomalies detected in the literature, represented in Figure 1, the following trend emerges: Anomaly AN05 stands out as the most recurrent, with a total of 112 references, representing 62.22% of the total references found in the literature, closely followed by AN08 with 107 references (59.44%). These two anomalies cover a significant portion of the vulnerability spectrum, indicating that they are critical areas requiring prioritized risk mitigation in cybersecurity. Similarly, anomalies such as AN10, AN04, AN03, and AN13 also show notable frequencies, with 64 (35.56%), 61 (33.89%), 57 (31.67%), and 43 (23.89%) references, respectively, suggesting that these also represent significant risks that should not be ignored. In contrast, anomalies like AN07 have a much lower presence, representing less than 3% of the total, suggesting a relatively limited impact compared to the primary identified threats. Finally, anomalies such as AN11, AN02, AN09, AN12, AN06, and AN01 have a moderate impact, with reference percentages ranging between 3.33% and 14.44%.

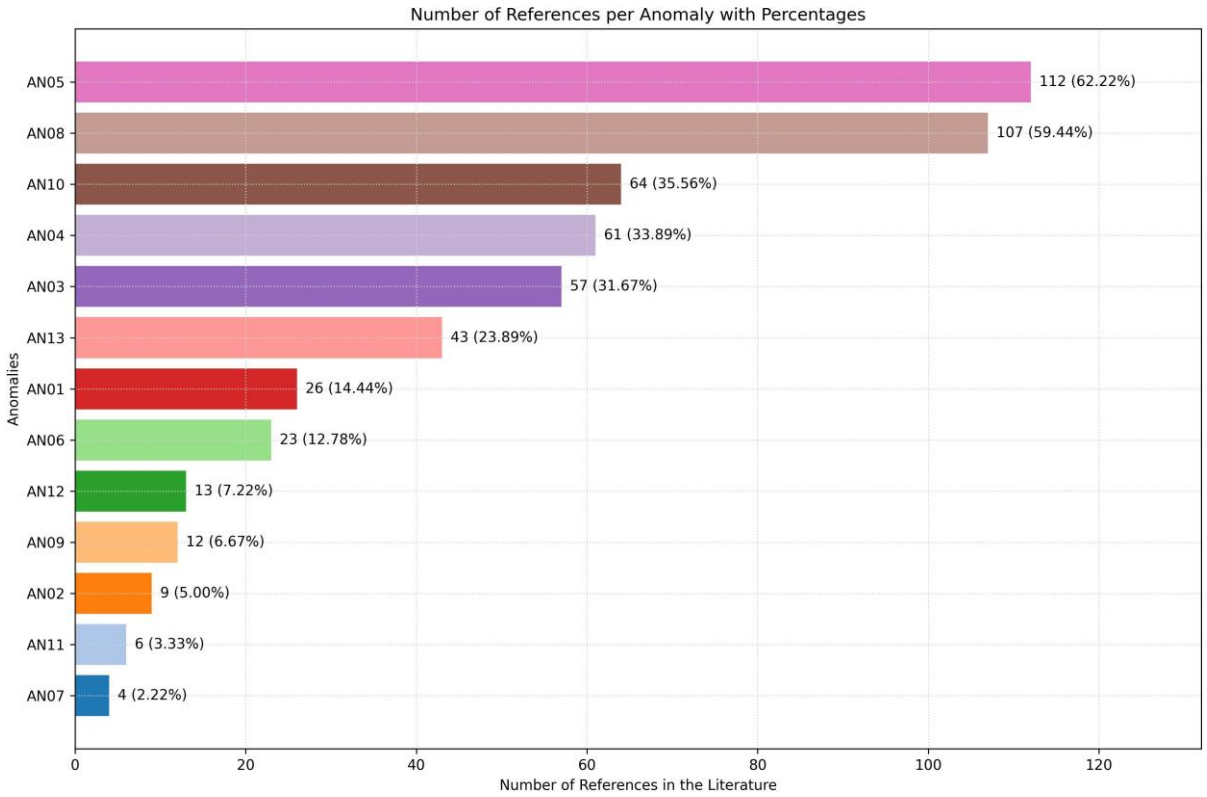

Figura 1. Number of References Cited per Anomaly with Corresponding Percentages

The study identified critical sectors in cybersecurity with high vulnerability and a need for prioritized attention, as shown in Table 7. These sectors present a high incidence of cyber threats, highlighting the urgency of implementing advanced protection measures. This identification has enabled a deeper understanding of specific risks and facilitated the development of more effective strategies to mitigate these risks and protect critical assets. This approach underscores the importance of cybersecurity in strategic areas and provides a

foundation for future research aimed at enhancing security in these environments. By focusing on the most vulnerable sectors, resource allocation and the design of more targeted security policies are optimized, which is essential for strengthening defenses against cyber threats in key sectors of the economy and infrastructure. The findings, illustrated in Table 7 and Figure 2, are fundamental for guiding the implementation of cyber defenses.

The analysis of vulnerable sectors in cybersecurity, represented in Figure 2, reveals that the Information and Communication Technology (ICT) sector is the most affected, with 13 anomalies (17.57%), followed by Telecommunications at 14.86% and Education at 12.16%. The Government and Automotive sectors each show an incidence of 10.81%. In contrast, sectors such as Energy (9.46%), Finance (8.11%), Health (6.76%), Retail (5.41%), and Manufacturing (4.05%) display a lower incidence of anomalies. These findings emphasize the importance of prioritizing cybersecurity in the most vulnerable sectors, while those less affected should strengthen their measures. Additionally, the analysis helps optimize resource allocation and design more precise security policies.

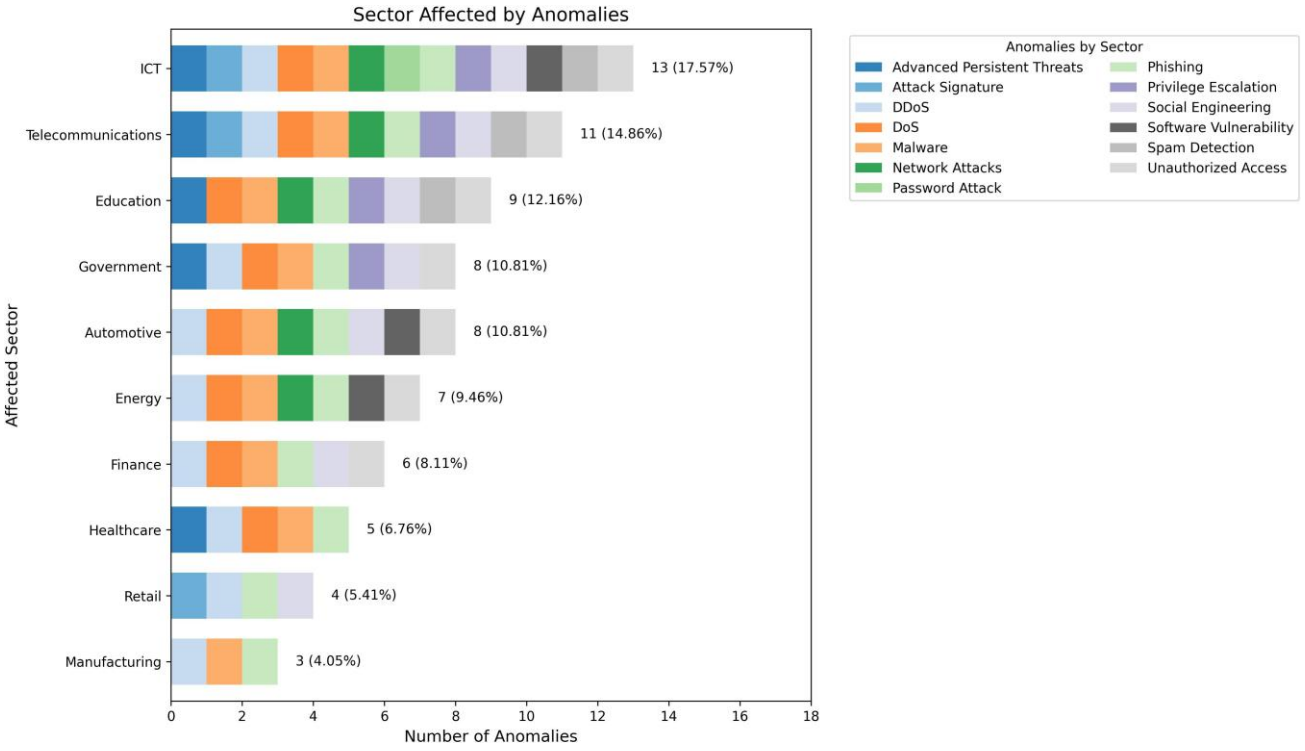

Figura 2. Sector-Wise Distribution of Anomalies and Their Corresponding Types

3.2 Q2. What are the most effective Machine Learning techniques used in cybersecurity within critical sectors, and what is their impact on enhancing digital security?

The systematic literature review (SLR) revealed various Machine Learning techniques applied to cybersecurity analysis, valued for their effectiveness in uncovering previously unknown relationships and patterns, which has enabled a deeper understanding of the investigated phenomena. These techniques have been fundamental in achieving the objectives outlined in the reviewed studies, contributing considerable value to the field. Additionally, they not only facilitated the discovery of new information but also opened up new research opportunities by revealing previously unexplored connections and correlations.

This focus on the use of Machine Learning techniques underscores the importance of innovation in the field of cybersecurity and ethical hacking, where the ability to detect, analyze, and mitigate cyber threats from large volumes of data has become a fundamental pillar. In these areas, Machine Learning not only enables the identification of suspicious patterns and network behavior anomalies but also facilitates the prediction and prevention of attacks, thereby enhancing the protection of critical systems and information confidentiality.

These tools allow researchers not only to confirm existing hypotheses but also to formulate new questions and explore uncharted areas, thus expanding the horizon of knowledge across various fields. The analysis techniques found in this research are presented in Table 8. On the other hand, the analysis of the techniques applied in the literature, represented in Figure 3, reveals a clear trend in the frequency of use of these techniques in recent research. Technique T01 stands out as the most utilized, with a total of 60 references, representing 33.33% of the total references, closely followed by T18, with 54 references (30.0%). These two techniques occupy a significant portion of the spectrum of applied methods, suggesting they are predominant approaches in current research and may be aligned with the most innovative and effective areas in anomaly analysis in cybersecurity. Other relevant techniques include T23 with 38 references (21.11%), T26 with 35 references (19.44%), and T04 with 34 references (18.89%), underscoring their importance and widespread use in literature. Techniques like T21 and T05 also show notable frequencies, with 28 references (15.56%) and 24 references (13.33%), respectively. This indicates that these techniques play an important role and may be associated with key areas of research. Conversely, techniques such as T08, T10, T16, T15, T12, and T22 show a lower frequency of use, with the first at 2.22% and the others at 1.67% each. This suggests that, while these techniques are present in the literature, their application is less common, possibly due to their focus on specific niches or lower effectiveness compared to the more widely used techniques.

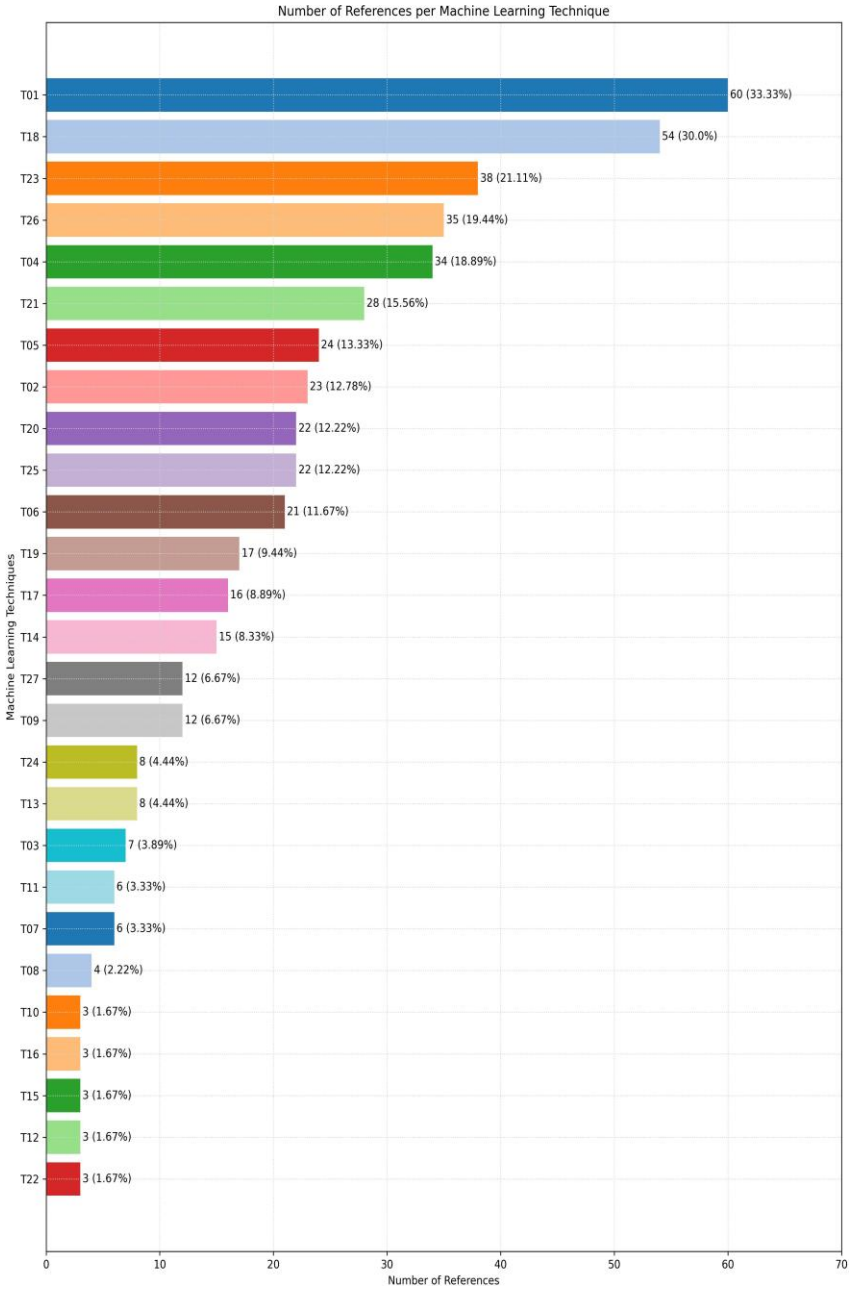

Figura 3. Number of References per Machine Learning Technique with Corresponding Percentages

Lastly, the different techniques found in the literature for risk detection and mitigation were analyzed for each identified anomaly. As shown in Figura 4, a cross-table of anomalies applied techniques, and references found in the SLR was created, which is presented in Table 9. The findings indicate that anomalies such as Phishing, Malware, and DoS, according to the literature, are mitigated through the application of 100% of the techniques identified in Table 8, suggesting these anomalies are extensively studied. Anomalies such as Social Engineering, Unauthorized Access, and DDoS are mitigated using more than 85% of the techniques identified in Table 9, which suggests that while they have been widely studied, there are still opportunities to incorporate additional techniques and deepen mitigation strategies. Anomalies like Advanced Persistent Threats, Spam Detection, and Network Attacks are mitigated using between 70.00% and 81.48% of the techniques identified, indicating a moderate level of study and suggesting potential for future research to expand the repertoire of applied techniques. Conversely, anomalies such as Attack Signature, Privilege Escalation, Software

Vulnerability, and Password Attack are mitigated with less than 60% and 3.7%, respectively, of the techniques identified in Table 9. This highlights a low level of study and emphasizes the need for further research efforts in these areas, exploring and applying a broader range of machine learning techniques for effective detection and mitigation.

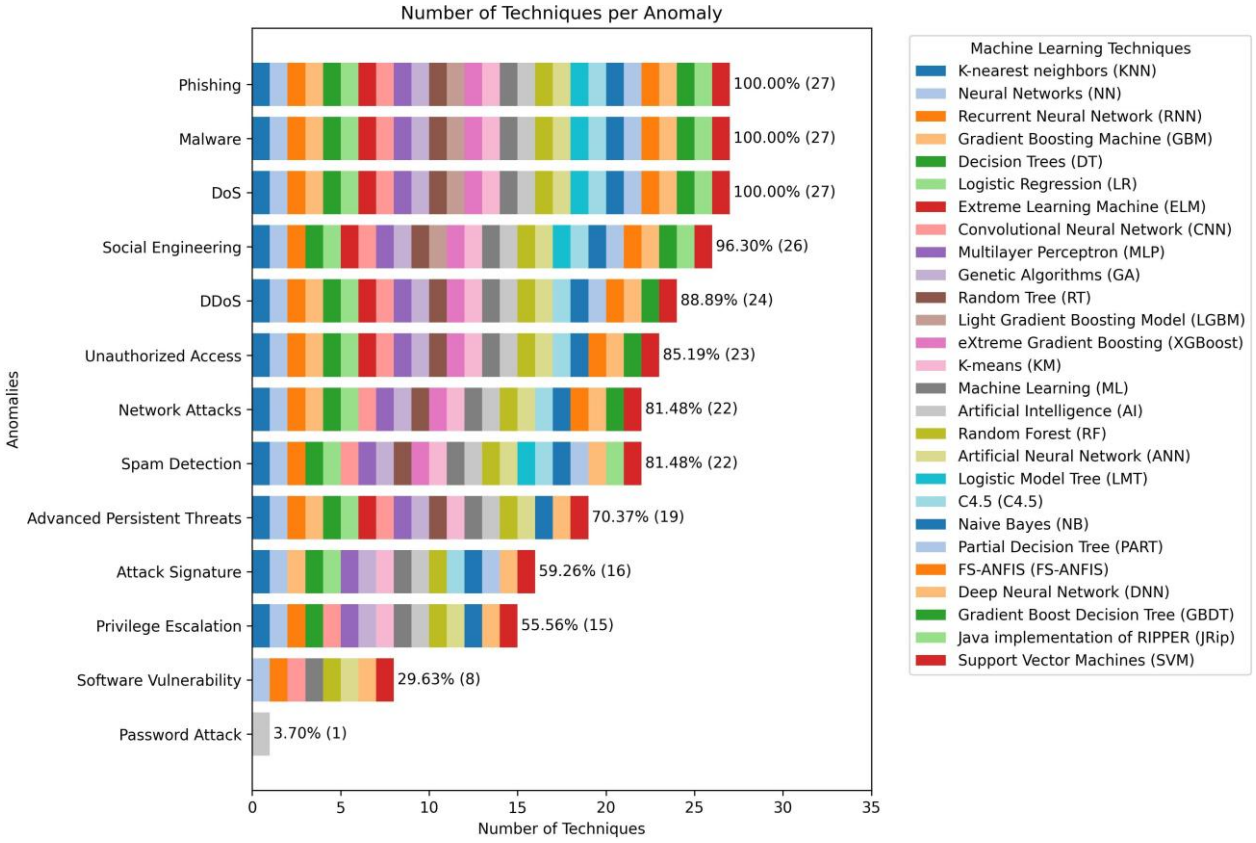

Figura 4. Number of Machine Learning Techniques by Anomalies with Corresponding Percentage

3.3 Q3. What are the ethical and legal implications of ethical hacking, and which regulatory frameworks are most suitable for each sector?

The ethical and legal implications of ethical hacking vary considerably across sectors, with a general focus on protecting privacy, data integrity, and regulatory compliance. Financial Sector: Regulations such as GDPR, ISO/IEC 27001, and PSD2 are essential to ensure systems respect user rights [23]; [6]; [9]; [13]; [15]; [18]; [24]; [25]; [26]; [27]; [28]; [29]; [30]; [31]; [32]; [33]; [34]; [35]; [36]; [37]. In cases of authorized push payment (APP) fraud, AI systems must be transparent and auditable [38]; [30]; [39]. In phishing, GDPR compliance mandates safeguarding privacy [40]; [31]; [41]; [42]; [43]; [44]. Healthcare Sector: Automated systems for phishing detection must comply with cybersecurity and data protection regulations [5]; [7]; [45]; [46]; [19]; [47] [48] [49]; [50]; [51]. Regulations like HIPAA and GDPR are fundamental for safeguarding sensitive patient data [52]; [33]; [53]; [30]; [54];[55]; [56]; [57]; [58]; [59]. These frameworks also ensure equitable access to blockchain-based healthcare systems, guaranteeing that all patients have equal rights to information protection [60]; [35]; [61]; [62]. Manufacturing Sector: In the manufacturing sector, robotic and autonomous systems raise ethical concerns regarding worker safety and industrial data protection. Standards like NERC CIP and ISO/IEC 27001 are essential to protect these systems against cyberattacks and ensure operational safety [63]; [64]; [65]; [66]; [67]; [68]; [69]; [70]; [71]; Cybersecurity professionals must manage vulnerabilities and comply with regulations such as ISO/IEC 27001 and IEC 62443 to prevent incidents and avoid legal penalties [72]. Educational Sector: In the educational sector, teaching about attacks on cyber-physical systems presents ethical and legal challenges. Institutions must educate without promoting malicious activities and comply with regulations like GDPR and the Data Protection Act to safeguard student privacy [73]; [74]; Pawlicka et al. (2023); [75]; [76]; [48]; [29]; [62]; [77]; [39]; [78]; [79]; [80]. Phishing exercises must be ethical

and controlled [81]. Universities should assess vulnerabilities using tools like Burp Suite and OWASP ZAP. Information Technology Sector: In the Information Technology sector, phishing detection must comply with GDPR and NIST [82]. Blockchain and AI in cybersecurity raise ethical and legal challenges, requiring transparency according to GDPR and NIST standards [83]; [84];[62]; [85]. Vulnerability testing should follow CVSS V3.1 [86]; [87].

Risk management and ethical hackers must comply with NIST, ISO standards [88]. Information and Communication Technology (ICT) Sector: IoT developers must ensure security and privacy by complying with relevant regulations [89]. NICS should be implemented responsibly and rigorously tested [90]. In cases of cybercrime and audio forensics, experts must handle evidence with precision and adhere to ethical and legal protocols to protect privacy and ensure admissibility in court [91]. Government Sector: In critical government infrastructure, ethical hacking must be conducted responsibly to ensure security and privacy. Promoting cybersecurity education and complying with standards like NIST and GDPR while adapting policies locally is essential [92]. In critical sectors such as energy, manufacturing, and telecommunications, security must not compromise essential operations [10]; [83]; [93]; [30]; [43]; [50]; [77]. Employee education and compliance with regulations such as the Personal Data Protection Act and ISO/IEC 27001 are necessary to safeguard sensitive information [94].

Telecommunications Sector: IoT technologies face ethical and legal challenges in data protection; compliance with GDPR and ISO/IEC 27001 is essential [1]; [95]; [96]; [97]; [32]; [98], utilizing intrusion detection and encryption, and also aligning with IEEE 802.11 [99]; [100]; [101] to safeguard infrastructure and data [31]; [102]. CVSS manages critical vulnerabilities [103]. ESASCF optimizes vulnerability assessments, complying with PCI-DSS, HIPAA, and ISO/IEC 27001 [104]. The NIST Cybersecurity Framework protects networks and adheres to GDPR [105]; [106]; phishing and cloaking detection must comply with GDPR and NIST [107]. Meeting specifications and ensuring interoperability prevent penalties [108]; detecting DoS attacks in Wi-Fi maintains service availability [109]. PYMEs Sector: They must ethically protect their data against cyberattacks, optimizing resources with tools like CENSOR [64].Legally, they must comply with the NIST Cybersecurity Framework, GDPR, and the NIS Directive [110]; [62]; [43]; [50]; [77]; [54]; [67], and follow NCSC guidelines to avoid penalties. In finance, compliance with GDPR and PSD2 is essential for fraud detection [111]. Low-cost automated audits improve cybersecurity and ISO/IEC 27001 compliance. The CYRVM platform promotes accessible ethical cyber risk management for SMEs [112]. In Bahrain, cybersecurity audits help prevent cybercrime and educate employees [113].

Automotive Sector: Vehicle manufacturers have an ethical responsibility to ensure the security of their systems and sensors against cyberattacks and to comply with cybersecurity standards such as ISO/IEC 27001. They must also secure Over-The-Air (OTA) software updates to maintain system safety against new threats [114]; [39]. These standards help protect users from failures or vulnerabilities in vehicles, ensuring continuous safety [16]; [115]; [42]; [62]; [32]; [34]; [58]. Energy Sector: In critical infrastructure, it is essential to use tools such as MITRE ATT&CK exclusively for protection [116]. Legal frameworks like NIST and the NIS Directive in Europe are crucial for defending against cyberattacks [117]; [83]; [118]; [40]; [61]; [32]; [119]; [65]; [66]; [57]; [69]. Responsible management of cyber threat intelligence (CTI) must comply with data protection and cybersecurity standards [120]; [121]; [122]; [123]. Energy infrastructures should adhere to frameworks like NERC CIP and ISO/IEC 27001 to protect operational data [63]; [31]; [43]; [82].

Transportation Sector: It is essential to manage cyber incidents in transportation and aviation promptly to protect operational and passenger safety [124]. Compliance with regulations from organizations like the International Maritime Organization (IMO), GDPR, and HIPAA helps prevent vulnerabilities and protects sensitive data in critical systems [125]; [126]; [52]; [127]; [54]; [35]; [58]; [124]. The use of networks like Tor raises ethical dilemmas; while it protects privacy, it can also be exploited for illicit activities, requiring regulatory frameworks that balance protection and abuse prevention [128].

3.4 Q4. What are the main gaps in current research on ethical hacking and trust-based testing, and how might the integration of emerging technologies, such as artificial intelligence, address these gaps?

The main gaps in current research on ethical hacking and trust-based testing include:
Lack of Standardization in Ethical Hacking and Trust-Based Testing: Ethical hacking tests require a standardized method to ensure they are conducted consistently and reliably, especially in critical sectors such as healthcare and telecommunications [1]; [2]; [23]; [6]; [38]; [17]; [129]; [24]; [130]; [74]; [131]; [125]; [31]; [55];

[33]. In phishing detection, convolutional neural network (CNN)-based methods still face inconsistencies due to the lack of a global standard [11]; [27]; [10]; [132]. Limitations in the Transferability of Machine Learning Models: Machine learning models are often highly specific to the data on which they were trained, making it challenging for them to perform well in new contexts [3]; [130]; [131], This is especially true in fields where data changes rapidly, such as healthcare and energy, [6].

Data Privacy and Trust Management in Collaborative Networks: Collaborative systems for intrusion detection face challenges in protecting privacy and establishing trust among their components [7]; [133]; [38]; [74]; [31]. Furthermore, limited interoperability between cybersecurity platforms remains a challenge in trust management [97]; [134]; [19]; [135]. Blockchain technology presents a potential solution to these challenges [13]; [18]; [121]; [63]; [136].

Lack of Integration of Ethical Hacking and Trust-Based Testing in Cyber-Physical Systems (CPS): These systems lack robust strategies to protect against advanced attacks [110]; [84]; [42]. Existing solutions face scalability issues due to high computational costs. The lack of integration of ethical hacking and trust-based testing hinders the proper evaluation of system resilience in real-world environments [76]; An and [31]; [82]. Limited Automation in Cyberattack Response: Many current systems lack automation in their responses to cyberattacks, which is crucial for mitigating the damage caused by advanced threats; [49]; [32]; [137]; [119]; [127]; [98]; [77]; [51]; [65]; [53]; [138]; [66]; Although some studies focus on detection mechanisms, the lack of integrated automated responses remains a significant gap. [34]; [85];

This lack of automation can lead to delayed responses, increasing the impact and potential damage of attacks. Limited Integration of AI in Emerging Threat Detection: AI has shown potential to enhance privacy and trust in distributed networks; however, its integration in emerging threat detection remains limited [121]; [40]; [52]; [44]. This is particularly relevant in collaborative environments, where the lack of AI-driven automation restricts systems' ability to dynamically adjust security levels [62]; [139]. Knowledge Transfer and Adaptability of AI: In phishing detection, feature selection and ensemble approaches, such as stacking, maintain high levels of accuracy, optimizing transfer between different datasets [5]; [6]; [9]; [15]. Lack of a Predictive Focus in Current Research on Ethical Hacking and Trust: Currently, cybersecurity research emphasizes reactive responses to cyber incidents rather than proactive anticipation.

Ethical hacking is typically employed after an attack has occurred [36], with limited exploration of artificial intelligence (AI) to predict and prevent cyberattacks. AI could detect anomalous behaviors and vulnerabilities in critical networks before they are exploited [37]; [140]; [70]. Dependence on Human Intervention: Various studies indicate that threat detection and response rely heavily on human intervention, limiting defense capabilities against attacks like phishing [78]. AI can automate this process, enabling faster reactions [141]. Absence of Dynamic and Personalized Models in Cybersecurity: Cybersecurity solutions need to be personalized according to user profiles [39]. As current approaches do not adapt to emerging real-time threats.

Dynamic and personalized AI-based models can optimize security by adjusting to user behavior and specific threats, reducing false positives and increasing defense efficiency [142]; [100]. Lack of Integration in Credential Management and Trust-Based Testing: There is a lack of personalized approaches in credential management and trust-based testing following security breaches; current systems do not adjust responses based on the risk level of compromised credentials [116]; [89]. Integrating AI could automate credential revocation and enable dynamic risk-based responses. Limitations in Scalability and Cost: While AI-based solutions are effective, large-scale adoption is limited by high costs [94]; [143]; [4], leaving organizations vulnerable.

There is a lack of AI in hybrid scenarios that address both physical and digital threats, representing a gap in the protection of critical infrastructure. Lack of AI Integration in Trust-Based Testing: NICS and HARMer face adoption and maturity challenges due to a lack of standardization and the complexity of intensive testing and configurations required in large networks [109]; [101]; [144]; [145]. AI could optimize these systems by automating customization and improving predictive capabilities [86]; [72]; [81]. The lack of predictive approaches leaves many organizations exposed to advanced cyberattacks [146]; [147]. Limitations in the Scalability of Security Solutions for Enterprise Networks: There are significant challenges in scaling cybersecurity solutions for large, complex enterprise networks [148]; [149]. AI-based approaches could improve efficiency by managing large data sets in real time and optimizing anomaly detection [79]; [80].

4. CONCLUSIONS

The integration of artificial intelligence in ethical hacking and trust-based testing is essential for enhancing cybersecurity and risk mitigation. AI facilitates knowledge transfer and model adaptability, allowing rapid adjustment to new contexts without requiring complete retraining. This is particularly relevant in critical areas such as phishing, where techniques like feature selection and ensemble methods, such as stacking, maintain high levels of accuracy when transferring knowledge across different datasets. The combination of blockchain and AI strengthens privacy and trust in threat detection, ensuring data authenticity and process transparency. In environments like IoT networks, this integration improves interoperability and enables more effective trust management. Furthermore, AI automates responses to cyberattacks, proactively blocking threats in real time and providing dynamic defense strategies that adjust to the evolving nature of risks. This allows organizations to dynamically adjust their security mechanisms, balancing data privacy and utility. Finally, AI enables continuous simulations of ethical hacking, allowing for ongoing assessment of cybersecurity robustness throughout an attack's lifecycle. This approach helps uncover vulnerabilities that might go unnoticed with traditional methods, significantly improving overall system security. Automation in attack planning and defense adaptation through advanced algorithms allows for the identification of complex attack patterns and dynamic adjustments in security responses. Therefore, the implementation of AI in penetration testing is crucial to enhancing the resilience of cyber systems, effectively anticipating and mitigating increasingly sophisticated threats.

5. ACKNOWLEDGMENT

The authors would like to thank the Servicio Nacional de Aprendizaje (SENA), Centro de Servicios y Gestión Empresarial – Antioquia Regional Office, for its institutional support and assistance in developing this research. Academic guidance and a commitment to applied research were fundamental to the consolidation of the results presented in this article.

6. AUTHORS' CONTRIBUTIONS

Paola Andrea Buitrago Cadavid and John Jairo Castro Maldonado contributed to the conceptualization and methodological design of the study, the development of the review protocol, the analysis and interpretation of the collected data, and the writing, review, and final consolidation of the manuscript. Bernardo De Jesús Zapata Baena and Robert David Urda Benítez contributed to the search, collection, screening, and segmentation of scientific information, supporting the selection, classification, and organization of the studies included in the review.

7. REFERENCIAS BIBLIOGRÁFICAS

[1] P. Danso, S. Dadkhah, E. Neto, A. Zohourian, H. Molyneaux, R. Lu, et al., "Transferability of machine learning algorithm for IoT device profiling and identification," IEEE Internet of Things Journal, vol. 11, pp. 2322–2335, 2024, doi: 10.1109/JIOT.2023.3292319.
[2] F. Santoso and A. Finn, "An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures," IEEE Transactions on Services Computing, vol. 17, pp. 1293–1307, 2024, doi: 10.1109/TSC.2023.3331083.
[3] F. Alsubaei, A. Almazroi, and N. Ayub, "Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics," IEEE Access, vol. 12, pp. 8373–8389, 2024, doi: 10.1109/ACCESS.2024.3351946.

[4] R. Hamon, H. Junklewitz, J. Garrido, and I. Sanchez, "Three challenges to secure AI systems in the context of AI regulations," IEEE Access, vol. 12, pp. 61022–61031, 2024, doi: 10.1109/ACCESS.2024.3391021.
[5] S. Barbaria, M. Mont, E. Ghadafi, H. Machraoui, and H. Rahmouni, "Leveraging patient information sharing using blockchain-based distributed networks," IEEE Access, vol. 10, pp. 106334–106350, 2022, doi: 10.1109/ACCESS.2022.3206046.

[6] L. Kalabarige, R. Rao, A. Pais, and L. Gabralla, “A boosting-based hybrid feature selection and multi-layer stacked ensemble learning model to detect phishing websites,” IEEE Access, vol. 11, pp. 71180–71193, 2023, doi: 10.1109/ACCESS.2023.3293649.
[7] K. Agrawal, M. Aggarwal, S. Tanwar, G. Sharma, P. Bokoro, and R. Sharma, “An extensive blockchain-based applications survey: Tools, frameworks, opportunities, challenges, and solutions,” IEEE Access, vol. 10, pp. 116858–116873, 2022, doi: 10.1109/ACCESS.2022.3219160.
[8] S. Javed, M. Ahmad, M. Asif, W. Akram, K. Mahmood, A. Das, et al., “APT adversarial defence mechanism for industrial IoT enabled cyber-physical system,” IEEE Access, vol. 11, pp. 74000–74017, 2023, doi: 10.1109/ACCESS.2023.3291599.
[9] R. Abdillah, Z. Shukur, M. Mohd, T. Zamri, I. Oh, and K. Yim, “Performance evaluation of phishing classification techniques on various data sources and schemes,” IEEE Access, vol. 11, pp. 38721–38734, 2023, doi: 10.1109/ACCESS.2022.3225971.
[10] H. Lee, S. Lee, K. Kim, and H. Kim, “Hsviz-II: Octet layered hierarchy simplified visualizations for distributed firewall policy analysis,” IEEE Access, vol. 12, pp. 936–948, 2024, doi: 10.1109/ACCESS.2023.3346922.
[11] F. Liang, W. Hatcher, W. Liao, W. Gao, and W. Yu, “Machine learning for security and the internet of things: The good, the bad, and the ugly,” IEEE Access, vol. 7, pp. 158126–158137, 2019, doi: 10.1109/ACCESS.2019.2948912.
[12] N. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, “Deep learning for phishing detection: Taxonomy, current challenges and future directions,” IEEE Access, vol. 10, pp. 36429–36445, 2022, doi: 10.1109/ACCESS.2022.3151903.
[13] S. Remya, M. Pillai, K. Nair, S. Subbareddy, and Y. Cho, “An effective detection approach for phishing URL using ResMLP,” IEEE Access, vol. 12, pp. 79367–79382, 2024, doi: 10.1109/ACCESS.2024.3409049.
[14] V. Mullet, P. Sondi, and E. Ramat, “A review of cybersecurity guidelines for manufacturing factories in Industry 4.0,” IEEE Access, vol. 9, pp. 23235–23251, 2021, doi: 10.1109/ACCESS.2021.3056650.
[15] J. Schoenherr, “Insider threats and individual differences: Intention and unintentional motivations,” IEEE Transactions on Technology and Society, vol. 3, pp. 175–184, 2022, doi: 10.1109/TTS.2022.3192767.
[16] M. Almehdhar, A. Albaseer, M. Khan, M. Abdallah, H. Menouar, S. Al-Kuwari, et al., “Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks,” IEEE Open Journal of Vehicular Technology, vol. 5, pp. 869–888, 2024, doi: 10.1109/OJVT.2024.3422253.
[17] L. Tidjon, M. Frappier, and A. Mammar, “Intrusion detection systems: A cross-domain overview,” IEEE Communications Surveys & Tutorials, vol. 21, pp. 3639–3661, 2019, doi: 10.1109/COMST.2019.2922584.
[18] T. Lewis and B. Rimal, “Effects of removing user-land hooks in endpoint protection during attack experiments,” IEEE Access, vol. 12, pp. 15820–15842, 2024, doi: 10.1109/ACCESS.2024.3357525.
[19] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid, et al., “BotDet: A system for real-time botnet command and control traffic detection,” IEEE Access, vol. 6, pp. 38947–38958, 2018, doi: 10.1109/ACCESS.2018.2846740.
[20] C. Grady, S. Rajtmajer, and L. Dennis, “When smart systems fail: The ethics of cyber–physical critical infrastructure risk,” IEEE Transactions on Technology and Society, vol. 2, pp. 6–13, 2021, doi: 10.1109/TTS.2021.3058605.
[21] A. Chorppath, T. Alpcan, and H. Boche, “Bayesian mechanisms and detection methods for wireless network with malicious users,” IEEE Transactions on Mobile Computing, vol. 15, pp. 2452–2463, 2016, doi: 10.1109/TMC.2015.2505724.
[22] Y. Lyu, H. Cho, P. Jung, and S. Lee, “A systematic literature review of issue-based requirement traceability,” IEEE Access, vol. 11, pp. 13334–13348, 2023.
[23] S. Marchal, J. François, R. State, and T. Engel, “PhishStorm: Detecting phishing with streaming analytics,” IEEE Transactions on Network and Service Management, vol. 11, pp. 458–471, 2014, doi: 10.1109/TNSM.2014.2377295.
[24] M. Jang and K. Lee, “An advanced approach for detecting behavior-based intranet attacks by machine learning,” IEEE Access, vol. 12, pp. 52480–52495, 2024, doi: 10.1109/ACCESS.2024.3387016.
[25] S. Kumar, S. Gupta, and S. Arora, “Research trends in network-based intrusion detection systems: A review,” IEEE Access, vol. 9, pp. 157761–157775, 2021, doi: 10.1109/ACCESS.2021.3129775.

[26] M. Hina, M. Ali, A. Javed, F. Ghabban, L. Khan, and Z. Jalil, “SEFACED: Semantic-based forensic analysis and classification of e-mail data using deep learning,” IEEE Access, vol. 9, pp. 98398–98411, 2021, doi: 10.1109/ACCESS.2021.3095730.

[27] I. Wiafe, F. Koranteng, E. Obeng, N. Assyne, A. Wiafe, and S. Gulliver, “Artificial intelligence for cybersecurity: A systematic mapping of literature,” IEEE Access, vol. 8, pp. 146598–146610, 2020, doi: 10.1109/ACCESS.2020.3013145.
[28] M. Marican, S. Razak, A. Selamat, and S. Othman, “Cyber security maturity assessment framework for technology startups: A systematic literature review,” IEEE Access, vol. 11, pp. 5442–5452, 2023, doi: 10.1109/ACCESS.2022.3229766.
[29] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, “A systematic literature review on phishing email detection using natural language processing techniques,” IEEE Access, vol. 10, pp. 65703–65719, 2022, doi: 10.1109/ACCESS.2022.3183083.
[30] Y. Fang, C. Zhang, C. Huang, L. Liu, and Y. Yang, “Phishing email detection using improved RCNN model with multilevel vectors and attention mechanism,” IEEE Access, vol. 7, pp. 81542–81554, 2019, doi: 10.1109/ACCESS.2019.2913705.
[31] D. Kim, M. Ahn, S. Lee, D. Lee, M. Park, and D. Shin, “Improved cyber defense modeling framework for modeling and simulating the lifecycle of cyber defense activities,” IEEE Access, vol. 11, pp. 114187–114200, 2023, doi: 10.1109/ACCESS.2023.3324901.
[32] F. Abri, J. Zheng, A. Namin, and K. Jones, “Markov decision process for modeling social engineering attacks and finding optimal attack strategies,” IEEE Access, vol. 10, pp. 109949–109964, 2022, doi: 10.1109/ACCESS.2022.3213711.
[33] B. Sun, T. Ban, C. Han, T. Takahashi, K. Yoshioka, J. Takeuchi, et al., “Leveraging machine learning techniques to identify deceptive decoy documents associated with targeted email attacks,” IEEE Access, vol. 9, pp. 87962–87971, 2021, doi: 10.1109/ACCESS.2021.3082000.
[34] F. Rosa, N. Maunero, P. Prinetto, F. Talentino, and M. Trussoni, “Threma: Ontology-based automated threat modeling for ICT infrastructures,” IEEE Access, vol. 10, pp. 116514–116531, 2022, doi: 10.1109/ACCESS.2022.3219063.
[35] J. Hu, S. Guo, X. Kuang, F. Meng, D. Hu, and Z. Shi, “I-HMM-based multidimensional network security risk assessment,” IEEE Access, vol. 8, pp. 1431–1442, 2020, doi: 10.1109/ACCESS.2019.2961997.
[36] N. Nejjari, K. Zkik, H. Hammouchi, M. Ghogho, and H. Benbrahim, “Assessing data breach factors through modern crime theory: A structural equation modeling approach,” IEEE Access, vol. 12, pp. 92198–92212, 2024, doi: 10.1109/ACCESS.2024.3423651.
[37] M. Zaoui, B. Yousra, S. Yassine, Y. Maleh, and K. Ouazzane, “A comprehensive taxonomy of social engineering attacks and defense mechanisms: Toward effective mitigation strategies,” IEEE Access, vol. 12, pp. 72224–72238, 2024, doi: 10.1109/ACCESS.2024.3403197.
[38] W. Meng, E. Tischhauser, Q. Wang, Y. Wang, and J. Han, “When intrusion detection meets blockchain technology: A review,” IEEE Access, vol. 6, pp. 10179–10188, 2018, doi: 10.1109/ACCESS.2018.2799854.
[39] A. Darem, A. Alhashmi, T. Alkhaldi, A. Alashjaee, S. Alanazi, and S. Ebad, “Cyber threats classifications and countermeasures in banking and financial sector,” IEEE Access, vol. 11, pp. 125138–125156, 2023, doi: 10.1109/ACCESS.2023.3327016.
[40] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. Latif, F. Al-Turjman, et al., “Cyber security threats detection in internet of things using deep learning approach,” IEEE Access, vol. 7, pp. 124379–124389, 2019, doi: 10.1109/ACCESS.2019.2937347.
[41] F. Sabry, W. Labda, A. Erbad, and Q. Malluhi, “Cryptocurrencies and artificial intelligence: Challenges and opportunities,” IEEE Access, vol. 8, pp. 175840–175855, 2020, doi: 10.1109/ACCESS.2020.3025211.
[42] D. Jibat, S. Jamjoom, Q. Al-Haija, and A. Qusef, “A systematic review: Detecting phishing websites using data mining models,” Intelligent and Converged Networks, vol. 4, pp. 326–341, 2023, doi: 10.23919/ICN.2023.0027.
[43] F. Heiding, B. Schneier, A. Vishwanath, J. Bernstein, and P. Park, “Devising and detecting phishing emails using large language models,” IEEE Access, vol. 12, pp. 42131–42144, 2024, doi: 10.1109/ACCESS.2024.3375882.
[44] S. Maroofi, M. Korczyński, A. Hölzel, and A. Duda, “Adoption of email anti-spoofing schemes: A large scale analysis,” IEEE Transactions on Network and Service Management, vol. 18, pp. 315–330, 2021, doi: 10.1109/TNSM.2021.3065422.
[45] A. Aloseel, H. He, C. Shaw, and M. Khan, “Analytical review of cybersecurity for embedded systems,” IEEE Access, vol. 9, pp. 961–975, 2021, doi: 10.1109/ACCESS.2020.3045972.

[46] K. Chen, F. Cao, L. Hao, M. Xiang, and M. M. Kamruzzaman, “Application analysis of digital neural network-based data mining method in maximizing the performance of sports training,” Rev. Bras. Med. Esporte, vol. 29, p. e2022_0152, 2023, doi: 10.1590/1517-8692202329012022_0152.

[47] S. Mohan, C. Thirumalai, and G. Srivastava, “Effective heart disease prediction using hybrid machine learning techniques,” IEEE Access, vol. 7, pp. 81542–81554, 2019, doi: 10.1109/ACCESS.2019.2923707.

[48] A. Yeboah-Ofori, S. Islam, S. Lee, Z. Shamszaman, K. Muhammad, M. Altaf, et al., “Cyber threat predictive analytics for improving cyber supply chain security,” IEEE Access, vol. 9, pp. 94318–94334, 2021, doi: 10.1109/ACCESS.2021.3087109.

[49] J. Ndibwile, E. Luhanga, D. Fall, D. Miyamoto, G. Blanc, and Y. Kadobayashi, “An empirical approach to phishing countermeasures through smart glasses and validation agents,” IEEE Access, vol. 7, pp. 130758–130771, 2019, doi: 10.1109/ACCESS.2019.2940669.

[50] A. Dimitriadis, E. Lontzetidis, B. Kulvatunyou, N. Ivezic, D. Gritzalis, and I. Mavridis, “Fronesis: Digital forensics-based early detection of ongoing cyber-attacks,” IEEE Access, vol. 11, pp. 728–743, 2023, doi: 10.1109/ACCESS.2022.3233404.

[51] M. Ayyash, T. Alsboui, O. Alshaikh, I. Inuwa-Dutse, S. Khan, and S. Parkinson, “Cybersecurity education and awareness among parents and teachers: A survey of Bahrain,” IEEE Access, vol. 12, pp. 86596–86613, 2024, doi: 10.1109/ACCESS.2024.3416045.

[52] Y. Huang, Y. Li, and Z. Cai, “Security and privacy in metaverse: A comprehensive survey,” Big Data Mining and Analytics, vol. 6, pp. 234–247, Jun. 2023, doi: 10.26599/BDMA.2022.9020047.

[53] S. Kalhoro, M. Rehman, V. Ponnusamy, and F. Shaikh, “Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review,” IEEE Access, vol. 9, pp. 99339–99362, 2021, doi: 10.1109/ACCESS.2021.3097144.

[54] S. Sai, U. Yashvardhan, V. Chamola, and B. Sikdar, “Generative AI for cyber security: Analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space,” IEEE Access, vol. 12, pp. 53497–53512, 2024, doi: 10.1109/ACCESS.2024.3385107.

[55] F. Djebbar and K. Nordström, “A comparative analysis of industrial cybersecurity standards,” IEEE Access, vol. 11, pp. 85315–85330, 2023, doi: 10.1109/ACCESS.2023.3303205.

[56] G. White, R. Allen, A. Samuel, A. Abdullah, and R. Thomas, “Antecedents of cyber-security implementation: A study of the cyber-preparedness of U.K. social enterprises,” IEEE Transactions on Engineering Management, vol. 69, pp. 3826–3837, 2022, doi: 10.1109/TEM.2020.2994981.

[57] F. Valenza, E. Karafili, R. Steiner, and E. Lupu, “A hybrid threat model for smart systems,” IEEE Transactions on Dependable and Secure Computing, vol. 20, pp. 4403–4417, 2023, doi: 10.1109/TDSC.2022.3213577.

[58] A. Ajmal, M. Shah, C. Maple, M. Asghar, and S. Islam, “Offensive security: Towards proactive threat hunting via adversary emulation,” IEEE Access, vol. 9, pp. 126023–126033, 2021, doi: 10.1109/ACCESS.2021.3104260.

[59] R. Marinho and R. Holanda, “Automated emerging cyber threat identification and profiling based on natural language processing,” IEEE Access, vol. 11, pp. 58915–58930, 2023, doi: 10.1109/ACCESS.2023.3260020.

[60] E. Alkeem, S. Kim, C. Yeun, M. Zemerly, K. Poon, G. Gianini, et al., “An enhanced electrocardiogram biometric authentication system using machine learning,” IEEE Access, vol. 7, pp. 123069–123075, 2019, doi: 10.1109/ACCESS.2019.2937357.

[61] F. Gallardo and A. Yuste, “SCER spoofing attacks on the Galileo open service and machine learning techniques for end-user protection,” IEEE Access, vol. 8, pp. 85515–85530, 2020, doi: 10.1109/ACCESS.2020.2992119.

[62] M. Keshk, B. Turnbull, E. Sitnikova, D. Vatsalan, and N. Moustafa, “Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems,” IEEE Access, vol. 9, pp. 55077–55089, 2021, doi: 10.1109/ACCESS.2021.3069737.

[63] T. Ustun, S. Farooq, and S. Hussain, “A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard,” IEEE Access, vol. 7, pp. 156044–156053, 2019, doi: 10.1109/ACCESS.2019.2948117.

[64] M. Tsiodra, S. Panda, M. Chronopoulos, and E. Panaousis, “Cyber risk assessment and optimization: A small business case study,” IEEE Access, vol. 11, pp. 44467–44480, 2023, doi: 10.1109/ACCESS.2023.3272670.

[65] M. Erendor and M. Yildirim, “Cybersecurity awareness in online education: A case study analysis,” IEEE Access, vol. 10, pp. 52319–52335, 2022, doi: 10.1109/ACCESS.2022.3171829.

[66] O. Falowo and J. Abdo, “2019–2023 in review: Projecting DDoS threats with ARIMA and ETS forecasting techniques,” IEEE Access, vol. 12, pp. 26759–26771, 2024, doi: 10.1109/ACCESS.2024.3367240.

[67] J. Nicholls, A. Kuppa, and N.-A. Le-Khac, “Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape,” IEEE Access, vol. 9, pp. 163965–163980, 2021, doi: 10.1109/ACCESS.2021.3134076.

[68] W. Syafitri, Z. Shukur, U. Mokhtar, R. Sulaiman, and M. Ibrahim, “Social engineering attacks prevention: A systematic literature review,” IEEE Access, vol. 10, pp. 39325–39340, 2022, doi: 10.1109/ACCESS.2022.3162594.

[69] K. Zheng, T. Wu, X. Wang, B. Wu, and C. Wu, “A session and dialogue-based social engineering framework,” IEEE Access, vol. 7, pp. 67781–67794, 2019, doi: 10.1109/ACCESS.2019.2919150.

[70] A. Alturki, N. Alshwihi, and A. Algarni, “Factors influencing players’ susceptibility to social engineering in social gaming networks,” IEEE Access, vol. 8, pp. 97383–97391, 2020, doi: 10.1109/ACCESS.2020.2995619.

[71] B. Zyoud and S. Lutfi, “The role of information security culture in zero trust adoption: Insights from UAE organizations,” IEEE Access, vol. 12, pp. 72420–72438, 2024, doi: 10.1109/ACCESS.2024.3402341.

[72] M. Slunjski, D. Sumina, S. Groš, and I. Erceg, “Off-the-shelf solutions as potential cyber threats to industrial environments and simple-to-implement protection methodology,” IEEE Access, vol. 10, pp. 114735–114748, 2022, doi: 10.1109/ACCESS.2022.3217797.

[73] P. Frontera and E. Rodríguez-Seda, “Network attacks on cyber–physical systems project-based learning activity,” IEEE Transactions on Education, vol. 64, pp. 110–116, 2021, doi: 10.1109/TE.2020.3014268.

[74] A. Battah, K. Salah, R. Jayaraman, I. Yaqoob, and A. Khalil, “Using blockchain for enabling transparent, traceable, and trusted university ranking systems,” IEEE Access, vol. 11, pp. 23792–23806, 2023, doi: 10.1109/ACCESS.2023.3253948.

[75] R. Liu, “Data analysis of educational evaluation using K-Means clustering method,” Computational Intelligence and Neuroscience, vol. 2022, pp. 1–10, Jul. 2022, doi: 10.1155/2022/3762431.

[76] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, “A survey of moving target defenses for network security,” IEEE Communications Surveys & Tutorials, vol. 22, pp. 1909–1940, 2020, doi: 10.1109/COMST.2020.2982955.

[77] H. Abroshan, J. Devos, G. Poels, and E. Laermans, “Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process,” IEEE Access, vol. 9, pp. 44928–44943, 2021, doi: 10.1109/ACCESS.2021.3066383.

[78] H. Aldawood and G. Skinner, “Analysis and findings of social engineering industry experts explorative interviews: Perspectives on measures, tools, and solutions,” IEEE Access, vol. 8, pp. 67321–67329, 2020, doi: 10.1109/ACCESS.2020.2983280.

[79] P. Jarupunphol, S. Seatun, and W. Buathong, “Measuring vulnerability assessment tools’ performance on the university web application,” Pertanika Journal of Science & Technology, vol. 31, pp. 2973–2993, 2023, doi: 10.47836/pjst.31.6.19.

[80] Y. Malhotra, “Bridging networks, systems, and controls frameworks for cybersecurity curricula standards development,” in 2015 NY Cyber Security Engineering Technology Association Conference, Rochester, NY, USA, 2015, doi: 10.21314/JOP.2018.201.

[81] J. Young and S. Farshadkhah, “Teaching tip: Hook, line, and sinker – the development of a phishing exercise to enhance cybersecurity awareness,” Journal of Information Systems Education, vol. 34, pp. 347–359, 2023, doi: 10.21125/jise.2023.347359.

[82] A. Nourian and S. Madnick, “A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet,” IEEE Transactions on Dependable and Secure Computing, vol. 20, pp. 1–18, 2023, doi: 10.1109/TDSC.2022.2509994.

[83] P. Dedousis, G. Stergiopoulos, G. Arampatzis, and D. Gritzalis, “Enhancing operational resilience of critical infrastructure processes through chaos engineering,” IEEE Access, vol. 11, pp. 106172–106185, 2023, doi: 10.1109/ACCESS.2023.3316028.

[84] A. Razaque, B. Alotaibi, M. Alotaibi, F. Amsaad, A. Manasov, S. Hariri, et al., “Blockchain-enabled deep recurrent neural network model for clickbait detection,” IEEE Access, vol. 10, pp. 3144–3159, 2022, doi: 10.1109/ACCESS.2021.3137078.

[85] N. Karim, O. Khashan, H. Kanaker, W. Abdulraheem, H. Alshinwan, and A.-K. Al-Banna, “Online banking user authentication methods: A systematic literature review,” IEEE Access, vol. 12, pp. 741–753, 2024, doi: 10.1109/ACCESS.2023.3346045.

[86] A. Masarweh and J. Al-Saraireh, “Threat led advanced persistent threat penetration test,” International Journal of Security and Networks, vol. 16, pp. 240–253, 2021, doi: 10.1504/IJSN.2022.10050431.

[87] P. Lachkov, L. Tawalbeh, and S. Bhatt, “Vulnerability assessment for applications security through penetration simulation and testing,” Journal of Web Engineering, vol. 21, pp. 2187–2208, 2022, doi: 10.13052/jwe1540-9589.2178.

[88] O. Keskin, K. Caramancion, I. Tatar, O. Raza, and U. Tatar, “Cyber third-party risk management: A comparison of non-intrusive risk scoring reports,” Electronics, vol. 10, p. 1168, 2021, doi: 10.3390/electronics10101168.

[89] A. Majumder, C. Veilleux, and J. Miller, “A cyber-physical system to detect IoT security threats of a smart home heterogeneous wireless sensor node,” IEEE Access, vol. 8, pp. 205989–206002, 2020, doi: 10.1109/ACCESS.2020.3037032.

[90] S. Shandilya, “Paradigm shift in adaptive cyber defense for securing the web data: The future ahead,” Journal of Web Engineering, vol. 21, pp. 1371–1376, 2022, doi: 10.13052/jwe1540-9589.21416.

[91] A. Singh and S. Lukose, “A recent advancement in techniques for investigating cybercrimes, digital crimes and audio forensics,” Indian Journal of Forensic Medicine and Pathology, vol. 14, pp. 739–742, 2021, doi: 10.21088/ijfmp.0974.3383.14321.46.

[92] M. Shah, F. Iqbal, U. Rehman, and P. Hung, “A comparative assessment of human factors in cybersecurity: Implications for cyber governance,” IEEE Access, vol. 11, pp. 87970–87982, 2023, doi: 10.1109/ACCESS.2023.3296580.

[93] J. Robertson, J. Fossaceca, and K. Bennett, “A cloud-based computing framework for artificial intelligence innovation in support of multidomain operations,” IEEE Transactions on Engineering Management, vol. 69, pp. 3913–3922, 2022, doi: 10.1109/TEM.2021.3088382.

[94] H. Choi, S. Park, and J. Kang, “Enhancing participatory security culture in public institutions: An analysis of organizational employees’ security threat recognition processes,” IEEE Access, vol. 12, pp. 47543–47556, 2024, doi: 10.1109/ACCESS.2024.3383311.

[95] I. Kandhro, S. Alanazi, F. Ali, A. Kehar, K. Fatima, M. Uddin, et al., “Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures,” IEEE Access, vol. 11, pp. 9136–9148, 2023, doi: 10.1109/ACCESS.2023.3238664.

[96] M. Eskandari, Z. Janjua, M. Vecchio, and F. Antonelli, “Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices,” IEEE Internet of Things Journal, vol. 7, pp. 6882–6894, 2020, doi: 10.1109/JIOT.2020.2970501.

[97] S. Torabi, A. Boukhtouta, C. Assi, and M. Debbabi, “Detecting internet abuse by analyzing passive DNS traffic: A survey of implemented systems,” IEEE Communications Surveys & Tutorials, vol. 20, pp. 3389–3410, 2018, doi: 10.1109/COMST.2018.2849614.

[98] T. Santhi and K. Srinivasan, “Chat-GPT based learning platform for creation of different attack model signatures and development of defense algorithm for cyberattack detection,” IEEE Transactions on Learning Technologies, vol. 17, pp. 1–12, 2024, doi: 10.1109/TLT.2024.3417252.

[99] P. Krishnamurthy, J. Kabara, and T. Anusas-amornkul, “Security in wireless residential networks,” IEEE Transactions on Consumer Electronics, vol. 48, pp. 157–166, 2002, doi: 10.1109/TCE.2002.1000199.

[100] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, “Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset,” IEEE Communications Surveys & Tutorials, vol. 18, pp. 184–211, 2016, doi: 10.1109/COMST.2015.2402161.

[101] H. Alipour, Y. Al-Nashif, P. Satam, and S. Hariri, “Wireless anomaly detection based on IEEE 802.11 behavior analysis,” IEEE Transactions on Information Forensics and Security, vol. 10, pp. 2158–2170, 2015, doi: 10.1109/TIFS.2015.2433898.

[102] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” Proceedings of the IEEE, vol. 104, pp. 1727–1765, 2016, doi: 10.1109/JPROC.2016.2558521.

[103] F. Jiang, D. Dong, L. Cao, and M. Frater, “Agent-based self-adaptable context-aware network vulnerability assessment,” IEEE Transactions on Network and Service Management, vol. 10, pp. 255–268, 2013, doi: 10.1109/TNSM.2013.090313.120388.

[104] M. Ghanem, T. Chen, M. Ferrag, and M. Kettouche, “ESASCF: Expertise extraction, generalization and reply framework for optimized automation of network security compliance,” IEEE Access, vol. 11, pp. 129840–129853, 2023, doi: 10.1109/ACCESS.2023.3332834.

[105] C. Griffy-Brown, H. Miller, V. Zhao, D. Lazarikos, and M. Chun, “Making better risk decisions in a new technological environment,” IEEE Engineering Management Review, vol. 48, pp. 77–84, 2020, doi: 10.1109/EMR.2020.2969121.

[106] J. Ragsdale and R. Boppana, “On designing low-risk honeypots using generative pre-trained transformer models with curated inputs,” IEEE Access, vol. 11, pp. 117528–117543, 2023, doi: 10.1109/ACCESS.2023.3326104.

[107] L. Tang and Q. Mahmoud, “A deep learning-based framework for phishing website detection,” IEEE Access, vol. 10, pp. 1509–1521, 2022, doi: 10.1109/ACCESS.2021.3137636.

[108] J. Song, C. Cadar, and P. Pietzuch, “SymbexNet: Testing network protocol implementations with symbolic execution and rule-based specifications,” IEEE Transactions on Software Engineering, vol. 40, pp. 695–711, 2014, doi: 10.1109/TSE.2014.2323977.

[109] M. Agarwal, S. Purwar, S. Biswas, and S. Nandi, “Intrusion detection system for PS-Poll DoS attack in 802.11 networks using real-time discrete event system,” IEEE/CAA Journal of Automatica Sinica, vol. 4, pp. 792–808, 2017, doi: 10.1109/JAS.2016.7510178.

[110] A. Emer, M. Unterhofer, and E. Rauch, “A cybersecurity assessment model for small and medium-sized enterprises,” IEEE Engineering Management Review, vol. 49, pp. 98–109, 2021, doi: 10.1109/EMR.2021.3078077.

[111] Y. Wei and Y. Sekiya, “Sufficiency of ensemble machine learning methods for phishing websites detection,” IEEE Access, vol. 10, pp. 124103–124113, 2022, doi: 10.1109/ACCESS.2022.3224781.

[112] P. Russo, A. Caponi, M. Leuti, and G. Bianchi, “A web platform for integrated vulnerability assessment and cyber risk management,” Information, vol. 10, p. 242, 2019, doi: 10.3390/info10070242.

[113] A. Almadhoob and R. Valverde, “Cybercrime prevention in the Kingdom of Bahrain via IT security audit plans,” Journal of Theoretical and Applied Information Technology, vol. 65, pp. 274–292, 2014.

[114] R. Heartfield, G. Loukas, and D. Gan, “You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks,” IEEE Access, vol. 4, pp. 6910–6925, 2016, doi: 10.1109/ACCESS.2016.2616285.

[115] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. Selvaraj, S. Plathottam, and P. Ranganathan, “Cybersecurity attacks in vehicular sensors,” IEEE Sensors Journal, vol. 20, pp. 13752–13765, 2020, doi: 10.1109/JSEN.2020.3004275.

[116] B. Al-Sada, A. Sadighian, and G. Olgieri, “Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database,” IEEE Access, vol. 12, pp. 1217–1233, 2024, doi: 10.1109/ACCESS.2023.3344680.

[117] D. Tayouri, N. Baum, A. Shabtai, and R. Puzis, “A survey of MulVAL extensions and their attack scenarios coverage,” IEEE Access, vol. 11, pp. 27974–27988, 2023, doi: 10.1109/ACCESS.2023.3257721.

[118] Y. Yang, Y. Li, Y. Shi, and D. Quevedo, “The vulnerability analysis of remote estimation with batch-data detectors against integrity attacks,” IEEE Transactions on Automatic Control, vol. 69, pp. 3096–3107, 2024, doi: 10.1109/TAC.2023.3332013.

[119] S. Bokhari and S. Myeong, “The influence of artificial intelligence on e-governance and cybersecurity in smart cities: A stakeholder’s perspective,” IEEE Access, vol. 11, pp. 69783–69796, 2023, doi: 10.1109/ACCESS.2023.3293480.

[120] M. Yusof, A. Almohammedi, V. Shepelev, and O. Ahmed, “Visualizing realistic benchmarked IDS dataset: CIRA-CIC-DoHBrw-2020,” IEEE Access, vol. 10, pp. 94624–94638, 2022, doi: 10.1109/ACCESS.2022.3204690.

[121] S. Gong, J. Cho, and C. Lee, “A reliability comparison method for OSINT validity analysis,” IEEE Transactions on Industrial Informatics, vol. 14, pp. 5428–5435, 2018, doi: 10.1109/TII.2018.2857213.

[122] G. Falco, C. Caldera, and H. Shrobe, “IIoT cybersecurity risk modeling for SCADA systems,” IEEE Internet of Things Journal, vol. 5, pp. 4486–4495, 2018, doi: 10.1109/JIOT.2018.2822842.

[123] P. Nespoli, F. Mármól, and J. Vidal, “A bio-inspired reaction against cyberattacks: AIS-powered optimal countermeasures selection,” IEEE Access, vol. 9, pp. 60971–60984, 2021, doi: 10.1109/ACCESS.2021.3074021.

[124] S. Enoch, Z. Huang, C. Moon, D. Lee, M. Ahn, and D. Kim, “Harmer: Cyber-attacks automation and evaluation,” IEEE Access, vol. 8, pp. 129397–129412, 2020, doi: 10.1109/ACCESS.2020.3009748.

[125] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke, “A holistic review of cybersecurity and reliability perspectives in smart airports,” IEEE Access, vol. 8, pp. 209802–209818, 2020, doi: 10.1109/ACCESS.2020.3036728.

[126] T. Kushal, K. Lai, and M. Illindala, “Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system,” IEEE Transactions on Smart Grid, vol. 10, pp. 4741–4750, 2019, doi: 10.1109/TSG.2018.2867809.

[127] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, “From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy,” IEEE Access, vol. 11, pp. 80218–80237, 2023, doi: 10.1109/ACCESS.2023.3300381.

[128] Z. Ling, J. Luo, K. Wu, W. Yu, and X. Fu, “Torward: Discovery, blocking, and traceback of malicious traffic over Tor,” IEEE Transactions on Information Forensics and Security, vol. 10, pp. 2515–2528, 2015, doi: 10.1109/TIFS.2015.2465934.

[129] A. Neupane, N. Saxena, J. Maximo, and R. Kana, “Neural markers of cybersecurity: An fMRI study of phishing and malware warnings,” IEEE Transactions on Information Forensics and Security, vol. 11, pp. 1969–1983, 2016, doi: 10.1109/TIFS.2016.2566265.

[130] W.-B. Hsieh, J.-S. Leu, and J.-I. Takada, “Use chains to block DNS attacks: A trusty blockchain-based domain name system,” Journal of Communications and Networks, vol. 24, pp. 347–356, 2022, doi: 10.23919/JCN.2022.000009.

[131] X. Koutsoukos, G. Karsai, A. Laszka, H. Neema, P. Volgyesi, Y. Vorobeychik, et al., “SURE: A modeling and simulation integration platform for evaluation of secure and resilient cyber–physical systems,” Proceedings of the IEEE, vol. 106, pp. 93–109, 2018, doi: 10.1109/JPROC.2017.2731741.

[132] C. Amrutkar, P. Traynor, and P. C. van Oorschot, “An empirical evaluation of security indicators in mobile web browsers,” IEEE Transactions on Mobile Computing, vol. 14, pp. 889–903, 2015, doi: 10.1109/TMC.2013.90.

[133] A. Shahid, A. Almogren, N. Javaid, F. Al-Zahrani, M. Zuair, and M. Alam, “Blockchain-based agri-food supply chain: A complete solution,” IEEE Access, vol. 8, pp. 69230–69243, 2020, doi: 10.1109/ACCESS.2020.2986257.

[134] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, “Explainable artificial intelligence in cybersecurity: A survey,” IEEE Access, vol. 10, pp. 93575–93586, 2022, doi: 10.1109/ACCESS.2022.3204171.

[135] E. S. Gualberto, R. T. de Sousa Jr., T. P. B. Vieira, J. P. C. L. da Costa, and C. G. Duque, “The answer is in the text: Multi-stage methods for phishing detection based on feature engineering,” IEEE Access, vol. 8, pp. 223529–223544, 2020, doi: 10.1109/ACCESS.2020.3043396.

[136] O. Sahingoz, E. Buber, and E. Kugu, “DePhIDes: Deep learning based phishing detection system,” IEEE Access, vol. 12, pp. 8052–8068, 2024, doi: 10.1109/ACCESS.2024.3352629.

[137] M. Ozkan-Okay, E. Akin, S. Kosunalp, T. Iliev, I. Stoyanov, et al., “A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions,” IEEE Access, vol. 12, pp. 12229–12243, 2024, doi: 10.1109/ACCESS.2024.3355547.

[138] K. Nimmy, S. Sankaran, K. Achuthan, and P. Calyam, “Lightweight and privacy-preserving remote user authentication for smart homes,” IEEE Access, vol. 10, pp. 176–187, 2022, doi: 10.1109/ACCESS.2021.3137175.

[139] X. Hu, D. Cheng, J. Chen, X. Jin, and B. Wu, “Multiontology construction and application of threat model based on adversarial attack and defense under ISO/IEC 27032,” IEEE Access, vol. 10, pp. 117955–117972, 2022, doi: 10.1109/ACCESS.2022.3220637.

[140] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, “Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior,” IEEE Access, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.

[141] M. Sahinoglu, “An input–output measurable design for the security meter model to quantify and manage software security risk,” IEEE Transactions on Instrumentation and Measurement, vol. 57, pp. 1251–1260, 2008, doi: 10.1109/TIM.2007.915139.

[142] G. Panigrahi, P. Sethy, S. Behera, M. Gupta, F. Alenizi, P. Suanpang, et al., “Analytical validation and integration of CIC-BELL-DNS-EXF-2021 dataset on security information and event management,” IEEE Access, vol. 12, pp. 83043–83056, 2024, doi: 10.1109/ACCESS.2024.3409413.

[143] G. Ahn, J. Jang, S. Choi, and D. Shin, “Research on improving cyber resilience by integrating the zero trust security model with the MITRE ATT&CK matrix,” IEEE Access, vol. 12, pp. 89291–89307, 2024, doi: 10.1109/ACCESS.2024.3417182.

[144] A. Alquwayzani, R. Aldossri, and M. Frikha, “Mitigating security risks in firewalls and web applications using vulnerability assessment and penetration testing (VAPT),” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 15, pp. 1348–1362, 2024, doi: 10.14569/IJACSA.2024.0150510.

[145] T. Caldwell, “Ethical hackers: Putting on the white hat,” Network Security, pp. 10–13, 2011, doi: 10.1016/S1353-4858(11)70078-2.

[146] Y. Nikoloudakis, I. Kefaloukos, S. Klados, S. Panagiotakis, E. Pallis, C. Skianis, et al., “Towards a machine learning based situational awareness framework for cybersecurity: An SDN implementation,” Sensors, vol. 21, p. 4939, 2021, doi: 10.3390/s21144939.

[147] S. Rehman, M. Mahmud, A. Rahman, I. Haq, and M. Safdar, “Information security in business: A bibliometric analysis of the 100 top cited articles,” Library Philosophy and Practice (e-journal), 2021. (sin DOI en tu fuente)

[148] D. Kongara and S. Krishnama, “A process of penetration testing using various tools,” Mesopotamian Journal of Cybersecurity, pp. 93–103, 2023, doi: 10.58496/MJCS/2023/014.

[149] B. Arfaj, S. Mishra, and M. Alshehri, “Efficacy of unconventional penetration testing practices,” Intelligent Automation & Soft Computing, vol. 31, pp. 224–239, 2022, doi: 10.32604/iasc.2022.019485.