Mustansiriyah Journal of Pure and Applied Sciences, Print ISSN: 2957-9910. Online ISSN: 2957-9929, Vol. 2, No. 4, 2024, Pages 126-139
DOI:

MJPAS

MUSTANSIRIYAH JOURNAL OF PURE AND APPLIED SCIENCES

Journal homepage:
https://mjpas.uomustansiriyah.edu.iq/index.php/mjpas

RESEARCH ARTICLE – Technical Engineering

A comprehensive Analysis of Approaches and Difficulties for Cybersecurity Threats-Article Review

Amer Mohamed Shhatha [1], Omar Ibrahim Alsaif [2*]

[1,2] Engineering Technical College- Mosul, Northern Technical University

[*] Corresponding author E-mail: omar.alsaif@ntu.edu.iq

Article Info.

Article history:

Received
30 March 2024

Accepted
21 April 2024

Publishing
30 September 2024

Abstract

This study delves deeply into numerous cybersecurity research endeavors, including rising fields such as IoT and connected vehicle security, as well as well-established dangers such as malware and DDoS assaults. Scholars use a variety of approaches, including deep learning and machine learning, with a strong emphasis on clear dataset descriptions and the consequences of false positives and negatives. The emphasis on accuracy and contextual awareness is very important, especially in IoT security. Rapid danger identification is primarily reliant on automation and efficacy, with a dedication to innovation demonstrated by the use of cutting-edge approaches such as Genetic and Wolf Optimization. However, striking a balance between feature selection, accuracy, and execution time remains a major difficulty. The availability of shared benchmark datasets facilitates comparable inquiries. Finally, the research intends to strengthen cybersecurity defenses and boost digital trust by providing essential insights and paths for navigating the ever-changing world of network protection.

The official journal published by the College of Education at Mustansiriya University

Keywords: Cybersecurity, Threat Detection, Machine Learning, Malware, Data Security.

1. Introduction

Similar examinations are made simpler by the accessibility of shared benchmark datasets. With an end goal to reinforce bunch guards and advance computerized trust, this review gives data and course to exploring the continuously changing network protection scene [1].

Facebook and other online business locales have flourished, and organizations and instructive establishments are embracing remote work and web-based learning. Yet, this change raises security issues, particularly with connection to shared internet-based work areas. Human mix-up in network safety stays a serious weakness notwithstanding solid specialized shields [2].

It is vital to teach representatives to lessen dangers like malware and hacking. Organizations need to send off mindfulness missions and set up innovative measures to forestall hazardous ways of behaving like overlooking secret phrase guidelines and leaving gadgets unattended [3][4].

Man-made brainpower (simulated intelligence), which reproduces human mental capacities with respect to information handling and navigation, has turned into a strong instrument in network safety [5]. Simulated intelligence empowered frameworks perform extraordinarily well at information examination, abnormality recognition, and digital danger anticipation, particularly in the period of 5G innovation, when information risk is expanded [6]..

Through the recognition of dubious examples, client approval check, and cybercrime forecast and counteraction, simulated intelligence-based methods further develop network safety. Danger alleviation and early interruption identification are enormously supported by these techniques [7]

This article stresses the meaning of profound learning and AI in network safety, showing their various purposes and analyzing how effective they are in obstructing interruptions and assaults. It is a valuable device for specialists, giving bits of knowledge into network protection patterns and approaches by drawing from dependable sources.

The article examines a wide range of cybersecurity research topics, from developing areas like the Internet of Things to well-established concerns like ransomware and DDoS assaults. The authors emphasize the need of adopting technologies like deep learning and machine learning, as well as providing explicit explanations of the data set and the ramifications of false positives and negatives. They emphasize the need of accuracy and contextual knowledge, particularly in terms of IoT security. The report emphasizes the need of promptly recognizing dangers through automation and efficiency, as well as a commitment to development by embracing cutting-edge technologies like Genetic and Wolf Optimization. The authors recognize the issue of balancing feature selection, accuracy, and execution time. They emphasize that having access to shared reference datasets makes it easier to conduct similar analyses. Finally, the essay intends to give insights and recommendations for navigating the ever-changing cybersecurity scene, with the ultimate goal of improving cybersecurity defenses and digital trust. This study adds to the area by synthesizing current research trends and approaches, serving as a valuable resource for both scholars and practitioners.

The article covers a wide range of cybersecurity concerns, beginning with an introduction that likely sets the tone for comprehending the following debates. It introduces the CIA Triad, which symbolizes the three fundamental cybersecurity principles: secrecy, integrity, and availability. This framework is essential for understanding the aims and objectives of cybersecurity efforts. The report then looks into many forms of cybersecurity and their functions, possibly covering topics such as network security, information security, and application security. Cybersecurity data science is most usually mentioned to emphasize the significance of data analysis in detecting and mitigating cyber threats. Furthermore, the report is anticipated to give an overview of malware assaults, including their nature, effect, and typical techniques used by attackers. It may also investigate malware detection strategies, categorizing them according to their methodology and efficacy. The use of machine learning in cybersecurity is expected to be researched, with a focus on anomaly detection, threat intelligence, and pattern identification. Finally, the article summarizes linked studies, most likely summarizing current research contributions and indicating gaps or opportunities for further investigation in the subject of cybersecurity. Overall, the article looks to provide a comprehensive summary of fundamental ideas, difficulties, and developments in cybersecurity, with useful insights for academics, practitioners, and educators.

2. Cybersecurity and CIA Triad

Cybersecurity is a critical field dedicated to safeguarding digital systems, networks, and data from unauthorized access, attacks, and breaches. It encompasses a wide range of measures, technologies, and practices aimed at protecting information assets and ensuring the confidentiality, integrity, and availability of digital resources. With the proliferation of interconnected devices and the increasing sophistication of cyber threats, cybersecurity has become more essential than ever. From securing personal devices to defending large-scale enterprise networks, cybersecurity professionals play a crucial role in identifying vulnerabilities, implementing preventive measures, and responding to cyber incidents effectively. In an age where digital transactions, communication, and operations are integral to daily life, robust cybersecurity measures are indispensable for maintaining trust, privacy, and security in the digital realm [8].

The idea known as the confidentiality, integrity and viability "CIA ", which is a foundation of data security. It comprises of three primary standards: accessibility, which ensures that frameworks and data are accessible and useful when required; uprightness, which safeguards the exactness and unwavering quality of information; and classification. These information stays private and open just to the people who are approved. These core values assist associations with getting against unapproved access, information control, and interferences to fundamental frameworks. They form the basis for the design and evaluation of security measures to protect assets and data as illustrate in Figure (1) [9].

A fundamental initial phase in aiding online protection groups characterize objectives is deciding the most ideal harmony between privacy, uprightness, and accessibility. Focusing on one security idea over another

every now and again involves compromises that could influence execution and speed. While an answer that totally keeps up with classification and respectability could function admirably in certain pieces of the economy, similar to medical care, it probably won't fill in too in different areas, similar to online business [10]. Table (1), Figure (2) and the following passages likewise give portrayals of the different parts of network safety.

Fig 1. The CIA triad [11].

Table 1. Cybersecurity Elements [12]

Element	Description
Infrastructure and network security	This concerns the most common way of guarding PC organizations, frameworks, and different assets against potential dangers, unapproved clients, and interruptions.
Application security	Investigating an application's source code to find and fix imperfections and weaknesses is known as application security. In a perfect world, security elements ought not be added as an idea in retrospect after the program has been sent off, yet rather ought to be integrated into the plan cycle.
Cloud security	The most common way of shielding distributed computing frameworks from blackouts, unlawful access, and cyberattacks is known as cloud security.
Information security	Data security is the method involved with shielding information during capacity or transmission to forestall unapproved access, burglary, or openness. Encryption, access controls, and other safety efforts are the fundamental accentuation of this space.
End user education	Further developing security mindfulness among end clients and authoritative staff requires end client training.
Disaster recovery	Debacle recuperation is the most common way of setting up methods and frameworks that let an organization manage unexpected conditions like blackouts, regular fiascoes, or cyberattacks.

Data security and network safety share common ground as they both address the protection of information on the internet. Online protection extends the practice of ensuring the confidentiality, integrity, and availability of data stored across various platforms, including organizations, computers, servers, and the cloud. In the present digital landscape, the majority of data is stored in digital formats, making robust security measures imperative [13]..

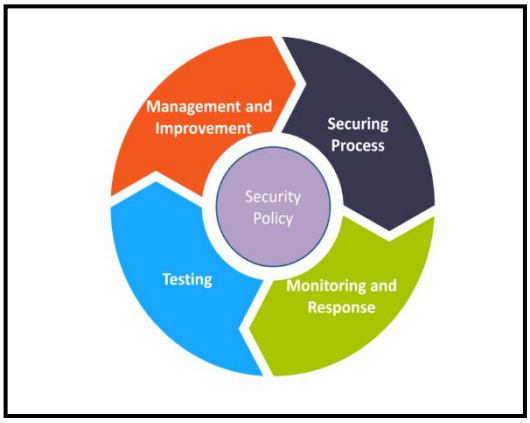

Fig 2. Cybersecurity components [9].

3. Types of Cybersecurity and Their Roles

The electronics developments and technology industry has grown significantly in the last several years, becoming indispensable in both the personal and professional domains. Due to the wide range of applications that modern devices run to support various facets of life, it is imperative that robust security measures be taken to guard against hacking, cyberattacks, intrusions, and unauthorized breaches. The constant threat of hacking and data theft is the main concern for many businesses and organizations, which is why they are stepping up their digital security measures [16].

There has been a significant shift towards cybersecurity measures as businesses from a variety of backgrounds become more conscious of the vital importance of their data. Cybersecurity is a multidimensional field that includes programs that restrict access to authorized persons only, data repositories, virtual and physical components of operating systems, and communication networks [[17]. Fundamentally, cybersecurity is a set of procedures and safeguards used to prevent harmful malware from entering a computer system and preserve its integrity [21]. Table (2) provides a summary of the many forms of cybersecurity and their functions in protecting computer systems.

Table 2. An outline of the different network protection types and their jobs in sustaining PC frameworks is introduced

Type	Key Function
Application Security	application of complex coding to protect and encrypt data in a way that is very difficult to crack[14].
Information Security	focuses on protecting data from unwanted access and alterations [15].
Infrastructure Security	safeguarding vital facilities, such data centers and electricity grids, and making sure there are no weaknesses [16].
Network Security	using technologies like two-factor authentication (2FA), remote access management, and efficient firewall techniques to protect networks from any invasions [17].
User Education	putting on educational seminars and conferences with a focus on cybersecurity experts and workers, increasing knowledge and readiness [16].

Figure (3) illustrates the sources of cyber threats. Three fundamental ideas are at the center of cybersecurity [20]. Beginning with secrecy guarantees that data inside a computer system can only be accessed and altered by those who are authorized. Second, data integrity prevents unwanted additions or removals. The last guarantee of availability is the reliable delivery of communications and data to the intended recipients, free from tampering or theft by unapproved parties[16].

Fig 3. Sources of cyber threats.

Cyberattacks have the potential to seriously disrupt organizations, impacting consumers, employees, and operations, irrespective of their source or intended recipient. Thus, in order to reduce potential dangers, it is imperative that staff members comprehend and follow the cybersecurity policies of their company. Table (3), lists prominent cyberattacks that should serve as warnings in the current digital age.

4. Cybersecurity Data Science

Data science is essential to many different domains, such as cybersecurity, commerce, and life sciences. Because of the strong reliance on data, it is especially important in the field of systems and cybersecurity. Analyzing security data—which can include files, documents, or user information on a network—is necessary to identify cyber threats. To trace the source of data entering a network, cybersecurity experts use methods like file hashes and custom criteria (such as signatures and heuristics). Although these manual methods have benefits, they need a lot of work to stay up to date with the always changing threat landscape [18]. Table (4) gives a summary of the several cybersecurity attacks, while Figure (4) shows how big data can be transformed into insights that can be put to use.

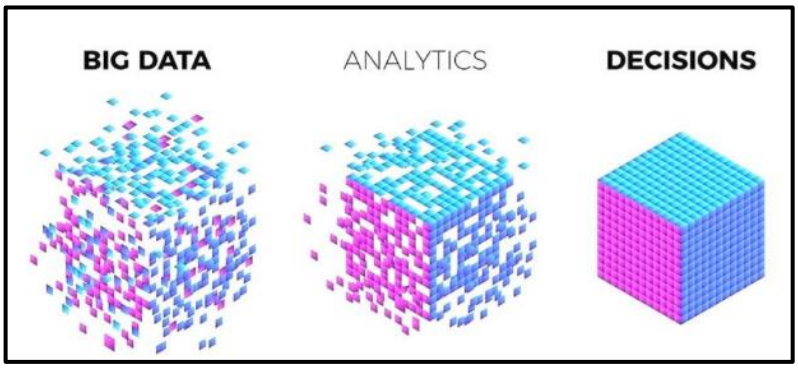

Fig 4. An exemplification of the process of data analysis [18]

Information technology could undergo a revolution thanks to data science. It looks for patterns and characteristics in training data to identify and fix system flaws using machine learning and deep learning techniques. Data science and artificial intelligence have gained popularity in cybersecurity in recent years as potent instruments for transforming unprocessed data into useful insights that support system security. Data science, which includes tasks like data engineering, volume reduction, pattern recognition, creation of novel security models, manipulation techniques to minimize false alarms, and resource optimization, essentially offers a more efficient way to make decisions [19]..

Table 4. Unmistakable Datasets Used in Network protection Exploration

Dataset	Description	Purpose and Applications
DARPA	The DARPA dataset incorporates IP association data among source and objective locations and comprises of LLDOS-1.0 and LLDOS-2.0.2 information [20].	Important for evaluating assault identification frameworks and interruption.
CAIDA	Includes ordinary traffic traces and distributed denial of service (DDoS) attack traffic, including data from DDoS attacks in 2007. assesses the machine [21].	Valuable for distinguishing DDoS assaults and further developing organization security.
CTU-13	A large dataset collected in 2011 from a Czech university that included background and regular traffic in addition to actual botnet traffic [22].	Empowers the turn of events and assessment of malware location frameworks.
KDD'99 Cup	A generally utilized dataset with 41 highlights for inconsistency recognition, classifying assaults into examining, R2L, U2R, and DoS beginning around 1999 [23].	Important for evaluating abnormality recognition and upgrading network security.
NSL-KDD	A popular dataset with 41 attributes that has been used since 1999 to identify anomalies, classify attacks into DoS, R2L, U2R, and probing [24].	Valuable for benchmarking interruption recognition models and frameworks.
MAWI	methods based on learning for identifying DDoS activity online [25].	Important for creating and testing traffic irregularity discovery procedures.
ISCX'12	This dataset, made by the Canadian Organization for Online protection, incorporates highlights for network entrance and AI based assault discovery models [26].	Ideal for assessing AI based interruption location and infiltration models.
Bot-IoT	Simulates Internet of Things scenarios in UNSW Canberra's Cyber Range Lab and includes a variety of attack files (e.g., DDoS, DoS, keylogging) [27].	Important for mimicking and testing security in IoT conditions.
ISOT'10	A combination of University of Victoria data flow that is harmful and that is not. Utilized for identifying assault areas, and classifying data using machine learning [28].	Reasonable for testing interruption recognition and grouping models.
UNSW-NB15	produced with the IXIA PerfectStorm tool at UNSW Canberra's Cyber Range Lab, featuring simulated attack actions and behaviors. includes 49 features for categorization and 9 assault types [29].	Ideal for assessing interruption location frameworks and concentrating on contemporary assault ways of behaving.

5. Malware Attack Analysis

As malware writers are always coming up with new ways to avoid detection, malware detection is a difficult process. Numerous malware detection methods have been developed by researchers; these can be broadly divided into three categories: machine learning, dynamic analysis, and static analysis. Analyzing the malware file itself without running it is known as static analysis [36]. Features including file size, file type, and the existence of known virus signatures can be extracted in this way. Using a sandbox environment to run the malware file and observe its behavior is known as dynamic analysis. This can be used to get features such system calls made, generated network traffic, and registry alterations [30].

It is possible to create a model to differentiate between benign and malicious files using machine learning techniques. Either static or dynamic analysis can be used to obtain features for the model to be trained. [31]. Table (5) summarizes the malware detection techniques proposed in seven recent research papers.

Table 5. Malware Detection Analysis

Author	Analysis	Design	Implementation	Testing
Huda et al. (2018) [32]	Malware behavior analysis using sandbox environment	Feature selection and extraction for malware detection	Wrapper-based detection engine	Test data evaluation
Narudin et al. (2016) [33]	Network traffic analysis for malware detection	Feature selection and extraction from network packets	Machine learning classifier training	Test data evaluation
Noor et al. (2018) [34]	Dynamic analysis of malware using Cuckoo sandbox	Execution profile generation	Malware behavior categorization	Test data evaluation
Talha et al. (2015) [35]	Static analysis of Android apps using APK Auditor	Malware detection based on app signature	App signature database	Test data evaluation
Ambusaidi et al. (2016) [36]	Network intrusion detection using least squares support vector machine (LS-SVM)	Feature selection and extraction from network packets	LS-SVM classifier training	Test data evaluation
Ali Mirza et al. (2018) [37]	Malware detection using machine learning	Feature selection and extraction from malware files	Machine learning classifier training	Test data evaluation
Tong & Yan (2017) [38]	Malware detection based on runtime system call patterns	System call pattern extraction	Malware pattern set and familiar pattern set generation	Test data evaluation

6. Malware Detection Techniques Classification

Techniques and tools for detecting and preventing malware infections are known as malware detection techniques. Malware is harmful software that has the ability to snoop on users, steal data, or harm or destroy computer systems. Techniques for detecting malware are crucial for defending computer systems against malware intrusions [38]. Table (6) below summarizes some of the most common malware detection techniques, their benefits and limitations.

Table 6. Malware Detection Techniques Classification [39][31]

Technique	Definition	Benefits	Limitations
Signature-based	Compares the malware to a database of known malware signatures.	Simple and fast, effective against most common malware.	Requires a frequently updated database, can be evaded by simple obfuscation techniques.
Behavior-based	Monitors the behavior of the malware while it is running to detect suspicious activity.	Can detect both known and unknown malware, including metamorphic malware.	Can be more complex and computationally expensive than signature-based detection, may generate false positives.
Statistical-based	Uses statistical analysis to identify patterns in malware that are not found in benign software.	Can detect metamorphic malware and other advanced malware.	Can be more complex and computationally expensive than signature-based detection, may generate false positives.
Heuristic-based	Uses machine learning and data mining techniques to identify malware based on its behavior and other characteristics.	Can detect both known and unknown malware, including metamorphic malware.	Can be complex and computationally expensive, may require a large dataset of malware samples to train the machine learning model.
Anomaly-based	Creates a model of normal system behavior and then uses that model to detect anomalous behavior that may indicate malware infection.	Can detect novel malware attacks that are not yet known to signature-based detection systems.	Can be complex and computationally expensive, may generate false positives.

7. Machine Learning in Cyber Security

The value of machine learning techniques in thwarting cybersecurity threats is becoming more widely acknowledged. These cover a wide range of issues, such as spam classification, fraud detection, phishing detection, malware detection, intrusion detection, and so forth. We focus on the domains of spam classification, intrusion detection systems, and malware detection in our analysis. Malware is a malicious code combination that is created with the goal to do harm and interfere with computer systems' regular operation [40].

Malware's main objective is to compromise digital assets and services' availability, integrity, and confidentiality by operating surreptitiously within a targeted system. In their exploration of the difficult terrain of applying machine learning algorithms for malware detection, Saad et al. have demonstrated their capacity to recognize new and polymorphic assaults. They contend that machine learning techniques will soon outperform conventional detection strategies, signaling a paradigm change in cybersecurity. They do, however, highlight the need of low-cost training methods for malware detection and the need for malware analysts to adjust and become skilled users of machine learning-driven malware detection methods [40][5].

At the same time, Ambalavanan and associates have given shrewd techniques to successfully distinguishing digital dangers. One huge downside of the security worldview is the basic job that typical clients play in evaluating the trustworthiness of PC assets, every now and again without the fundamental specialized skill. Cybercriminals utilize an extensive variety of assault procedures to exploit this weakness, like flooding assaults, malware penetration, unapproved information control, man-in-the-center (MiTM) attacks, replay assaults, pantomime, certifications spillage, secret key speculating, and the feared refusal of administration (DoS) and disseminated forswearing of administration (DDoS) attacks, to specify a couple. It becomes fundamental to have solid security principles to counter these assaults appropriately. AI models (ML calculations) can gain proficiency with the nuances of cyberattacks in both disconnected and online modes by utilizing datasets that have been reviewed and pre-handled. These calculations go about as careful sentinels, ready to detect marks of interruption, perceive dangers progressively, and act rapidly to safeguard advanced resources [41].

8. Summary of Results

An outline of a few explorations deals with online protection and danger recognition might be seen as in Table (7). These investigations cover a wide range of objectives, approaches, and discoveries, for the most part concerning Web of Things (IoT) security, associated auto dangers, and Conveyed Refusal of Administration (DDoS) attacks. The primary objectives of each study are illustrated, alongside any important datasets, procedures utilized, results achieved, solid areas, and exploration holes. The table capabilities as a careful asset, enlightening the different procedures and hardships in the continuously changing field of online protection danger recognizable proof and moderation.

Table 7. Literature Survey

Researcher	Techniques Used	Evaluation Metrics	Findings	Limitations
(Shamsolmoali and Zareapoor 2014) [42]	Factual procedure	Precise location of up to 97% of TCP assaults	Powerful in distinguishing TCP assaults	Restricted data on different sorts of DDoS assaults
(Xiao et al. 2015) [43]	CKNN with interface investigation	Further developed exactness through interface data utilization	Improved precision through interface examination	Absence of dataset subtleties
(Vrizlynn L. L. Thing 2017) [44]	Stacked autoencoder model	Robotization of component determination and arrangement	Productive abnormality discovery utilizing Weka apparatus	Explicit conversation on clever assault characterization missing
(Kushwah and Ali 2018) [45]	Counterfeit Brain Organizations with dark opening improvement	Not indicated	Use of improvement calculations for ANN preparing	Subtleties on the ANN construction and it are missing to prepare process
(Khalaf et al. 2019) [46]	Bayesian organizations, fluffy rationale, hereditary calculations, K-NN.	Not determined	Inside and out survey of different strategies and arrangement of DDoS assaults	Absence of subtleties on unambiguous datasets utilized
(Kushwah and Ranga 2020) [47]	V-ELM and examination with other ML calculations	Not indicated	Near investigation of V-ELM with other ML calculations	Dataset qualities are not given
(Ullah and Mahmoud 2020) [48]	Crossover model with choice tree and RF	Constant location and characterization	Center around tumultuous particles for development	Explicit difficulties progressively location not referenced
(G. Mohamed Amer 2021) [49]	DL for security data the board	Decreasing bogus alarms in irregularity discovery	Use of improvement calculations for ANN preparing	Influence on evident and misleading cautions not nitty gritty
(M. N. R. Khan et al 2022) [1]	Half and half ML strategy	Upgraded location of assailant avoidance	Near investigation of V-ELM with other ML calculations	Explicit avoidance techniques and their location not tended to
(J. Bharadiya 2023) [41]	Machine Learning in Cybersecurity	Not indicated	Using dfifferent technologies	Dataset qualities are not given

The comparison of numerous research papers on cybersecurity strategies provides useful discussion points about their methodologies, conclusions, and limits. Shamsolmoali and Zareapoor (2014) acquired a remarkable precision of up to 97% in TCP attack detection with a realistic technique, demonstrating its usefulness in this arena. However, their research was largely concerned with TCP attacks, leaving a vacuum in understanding other forms of DDoS attacks.

Similarly, Xiao et al. (2015) improved accuracy via interface analysis, although the absence of specific dataset information prevents a thorough evaluation of their technique. Vrizlynn L. L. Thing (2017) used a stacked autoencoder model to automate feature selection, resulting in effective anomaly detection; nevertheless, additional discussion of intelligent attack classification might improve the findings.

Kushwah and Ali (2018) used Artificial Brain Networks with black hole optimization, although the lack of specific assessment criteria and training procedure information restricts the reproducibility of their findings.

Khalaf et al. (2019) presented a thorough examination of numerous methodologies, however the lack of clarification on evaluation measures and dataset characteristics limits the application of their results. Kushwah and Ranga (2020) compared V-ELM to various ML algorithms, indicating its promise; nevertheless, dataset features were not supplied for a complete evaluation.

Ullah and Mahmoud (2020) concentrated on continuous detection and classification, emphasizing improvement tactics rather than directly tackling real-time issues. G. Mohamed Amer (2021) used deep learning to minimize false alarms in anomaly detection, however the influence on true and false alerts remains unclear. M. N. R. Khan et al. (2022) offered a hybrid ML methodology for attacker identification and prevention; however the exact prevention approaches and detection methods were not described. Finally, J. Bharadiya (2023) investigated Machine Learning in Cybersecurity but did not include dataset features, making it difficult to assess the generalizability of their findings.

Overall, while each research adds useful insights into cybersecurity strategies, addressing the interrelationships between these studies and other methodology would provide a more complete knowledge of the area.

Conclusions

This gathering's assessment of network safety research offers an intensive summation of the nonstop battle to guard computerized conditions against different assaults. Scientists have shown a commitment to further developing danger location procedures, handling both new and developing dangers like the Web of Things (IoT) and connected vehicles, as well as additional conventional perils like malware and Conveyed Forswearing of Administration (DDoS) attacks.

One essential finding is the range of approaches used to further develop danger identification: from factual techniques and inventive half and half models to AI and profound learning calculations. This outlines how complex network protection issues are. Numerous studies stress automation and efficiency, emphasizing the need of automated feature selection and classification for quick danger identification. Novel aspects like the LuNet model, stacked auto encoders, and genetic wolf optimization have been introduced by researchers, indicating continuous innovation. Improving threat detection involves trade-offs and obstacles, such as balancing execution time, accuracy, and feature selection.

Utilizing common benchmark datasets such as UNSW-NB15 and KDD Cup makes comparative analysis easier and advances the field. This research provides important insights for bolstering collective cybersecurity defenses in an ever-evolving cyber threat landscape. The fundamental objective is still to become resilient and adaptable in this changing environment. Through the utilization of varied approaches and the resolution of research gaps, the cybersecurity community has improved its ability to effectively negotiate intricate security concerns.

Acknowledgement

Authers would like to thank North Technical university for support.

Reference

[1] P. Sornsuwit and S. Jaiyen, “A New Hybrid Machine Learning for Cybersecurity Threat Detection Based on Adaptive Boosting,” *Appl. Artif. Intell.*, vol. 33, no. 5, pp. 462–482, 2019, doi: 10.1080/08839514.2019.1582861.

[2] G. Mohamed Amer, E. Abd El Hay, I. Abdel-Baset, and M. Abd El Azim Mohamed, “Development Machine Learning Techniques to Enhance Cyber Security Algorithms. (Dept. E),” *MEJ. Mansoura Eng. J.*, vol. 46, no. 4, pp. 36–46, 2021, doi: 10.21608/bfemu.2021.206401.

[3] R. Das and R. Sandhane, "Artificial Intelligence in Cyber Security," *J. Phys. Conf. Ser.*, vol. 1964, no. 4, 2021, doi: 10.1088/1742-6596/1964/4/042072.

[4] M. Wazid, A. K. Das, V. Chamola, and Y. Park, "Uniting cyber security and machine learning: Advantages, challenges and future research," *ICT Express*, vol. 8, no. 3, pp. 313–321, 2022, doi: 10.1016/j.icte.2022.04.007.

[5] D. M. B. Professor, V. Chancellor, Dr. Vivek Kumar, P. (Dr. . R. Singh, and P. (Dr. . B. K. Sarkar, *Cyber Security using Machine Learning*. Atlantis Press International BV, 2022. doi: 10.56962//9789355451170.

[6] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.

[7] M. Manjula, Venkatesh, and K. R. Venugopal, "Cyber Security Threats and Countermeasures using Machine and Deep Learning Approaches: A Survey," *J. Comput. Sci.*, vol. 19, no. 1, pp. 20–56, 2023, doi: 10.3844/jcssp.2023.20.56.

[8] P. Bagó, "Cyber security and artificial intelligence," *Econ. Financ.*, vol. 10, no. 2, pp. 189–212, 2023, doi: 10.33908/ef.2023.2.5.

[9] W. Nwankwo and K. C. Ukaoha, "Socio-technical perspectives on cybersecurity: Nigeria's cybercrime legislation in review," *Int. J. Sci. Technol. Res.*, vol. 8, no. 10, pp. 47–58, 2019.

[10] L. O. Nweke, "Using the CIA and AAA Models to Explain Cybersecurity Activities," *PM World J.*, vol. VI, no. Xii, pp. 1–3, 2017.

[11] Haaga-Helia, "Secure web development Pankaj Pant," *Haaga-Helia Univ. Appl. Sci.*, no. 8.5.2017, pp. 2003–2005, 2022.

[12] A. A. Alobaidi and N. B. Al Dabbagh, "Web Attacks and Defenses," *J. Educ. Sci.*, vol. 32, no. 2, pp. 91–100, 2023, doi: 10.33899/edusj.2023.137855.1319.

[13] A. M. Kovács, "Here there be Dragons: Evolution, Potentials and Mitigation Opportunities of Cybercrime in Nigeria A Review, Analysis, and Evaluation," *J. Cent. East. Eur. African Stud.*, pp. 0–1, 2021.

[14] A. Frankó, G. Hollósi, D. Ficzere, and P. Varga, "Applied Machine Learning for IIoT and Smart Production—Methods to Improve Production Quality, Safety and Sustainability," *Sensors*, vol. 22, no. 23, 2022, doi: 10.3390/s22239148.

[15] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M. Shah, and A. Anjum, "Data hiding technique in steganography for information security using number theory," *J. Inf. Sci.*, vol. 45, no. 6, pp. 767–778, 2019, doi: 10.1177/0165551518816303.

[16] G. Hale and C. Bartlett, “Managing the Regulatory Tangle: Critical Infrastructure Security and Distributed Governance in Alberta’s Major Traded Sectors,” *J. Borderl. Stud.*, vol. 34, no. 2, pp. 257–279, 2019, doi: 10.1080/08865655.2017.1367710.

[17] Y. Wang, A. Smahi, H. Zhang, and H. Li, “Towards Double Defense Network Security Based on Multi-Identifier Network Architecture,” *Sensors*, vol. 22, no. 3, pp. 1–17, 2022, doi: 10.3390/s22030747.

[18] M. M. Mijwil, I. E. Salem, and M. M. Ismaeel, “The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review,” *Iraqi J. Comput. Sci. Math.*, vol. 4, no. 1, pp. 87–101, 2023, doi: 10.52866/ijcsm.2023.01.01.008.

[19] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, “Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey,” *Electron.*, vol. 12, no. 8, pp. 1–18, 2023, doi: 10.3390/electronics12081920.

[20] Huda R. Shakir1,Sadiq A. Mehdi2, Anwar A. Hattab," A New Method for Color Image Encryption Using Chaotic System and DNA Encoding",Mustansiriyah Journal of Pure and Applied Sciences, Vol. 1, No.1(2023) 68-79

[21] M. P. Singh and A. Bhandari, “New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges,” *Comput. Commun.*, vol. 154, pp. 509–527, 2020, doi: 10.1016/j.comcom.2020.02.085.

[22] J. L. G. Torres, C. A. Catania, and E. Veas, “Active learning approach to label network traffic datasets,” *J. Inf. Secur. Appl.*, vol. 49, p. 102388, 2019, doi: 10.1016/j.jisa.2019.102388.

[23] S. Choudhary and N. Kesswani, “Analysis of KDD-Cup’99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT,” *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 1561–1573, 2020, doi: 10.1016/j.procs.2020.03.367.

[24] L. Dhanabal and S. P. Shantharajah, “A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms,” *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 6, pp. 446–452, 2015, doi: 10.17148/IJARCCE.2015.4696.

[25] B. Bouyeddou, F. Harrou, B. Kadri, and Y. Sun, “Detecting network cyber-attacks using an integrated statistical approach,” *Cluster Comput.*, vol. 24, no. 2, pp. 1435–1453, 2021, doi: 10.1007/s10586-020-03203-1.

[26] M. Idhammad, K. Afdel, and M. Belouch, “Semi-supervised machine learning approach for DDoS detection,” *Appl. Intell.*, vol. 48, no. 10, pp. 3193–3208, 2018, doi: 10.1007/s10489-018-1141-2.

[27] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, “Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset,” *Futur. Gener. Comput. Syst.*, vol. 100, pp. 779–796, 2019, doi: 10.1016/j.future.2019.05.041.

[28] I. H. Sarker, “Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep

Learning Perspective," *SN Comput. Sci.*, vol. 2, no. 3, 2021, doi: 10.1007/s42979-021-00535-6.

[29] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *J. Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00379-6.

[30] M. Naseer *et al.*, "Malware Detection: Issues and Challenges," *J. Phys. Conf. Ser.*, vol. 1807, no. 1, 2021, doi: 10.1088/1742-6596/1807/1/012011.

[31] S. Vasoya, K. Bhavsar, and N. Patel, "A systematic literature review on Ransomware attacks," *arXiv2212.04063v1 [cs.CY] 8 Dec 2022 Krishnaben*, 2022, [Online]. Available: http://arxiv.org/abs/2212.04063

[32] B. A. Oluwagbemiga, B. Shuib, S. J. Abdulkadir, and A. S. Hashim, "A hybrid multi-filter wrapper feature selection method for software defect predictors," *Int. J. Supply Chain Manag.*, vol. 8, no. 2, pp. 916–922, 2019.

[33] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," *Soft Comput.*, vol. 20, no. 1, pp. 343–357, 2016, doi: 10.1007/s00500-014-1511-6.

[34] M. Noor, H. Abbas, and W. Bin Shahid, "Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis," *J. Netw. Comput. Appl.*, vol. 103, pp. 249–261, 2018, doi: https://doi.org/10.1016/j.jnca.2017.10.004.

[35] A. T. Kabakus, İ. Doğru, and A. Çetin, "APK Auditor: Permission-based Android malware detection system," *Digit. Investig.*, vol. 13, Jun. 2015, doi: 10.1016/j.diin.2015.01.001.

[36] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE Trans. Comput.*, vol. 65, no. 10, pp. 2986–2998, 2016, doi: 10.1109/TC.2016.2519914.

[37] Q. K. Ali Mirza, I. Awan, and M. Younas, "CloudIntell: An intelligent malware detection system," *Futur. Gener. Comput. Syst.*, vol. 86, pp. 1042–1053, 2018, doi: 10.1016/j.future.2017.07.016.

[38] F. Tong and Z. Yan, "A hybrid approach of mobile malware detection in Android," *J. Parallel Distrib. Comput.*, vol. 103, pp. 22–31, 2017, doi: 10.1016/j.jpdc.2016.10.012.

[39] S. G. Kene and D. P. Theng, "A review on intrusion detection techniques for cloud computing and security challenges," *2nd Int. Conf. Electron. Commun. Syst. ICECS 2015*, no. February 2015, pp. 227–232, 2015, doi: 10.1109/ECS.2015.7124898.

[40] M. N. R. Khan, J. Ara, S. Yesmin, and M. Z. Abedin, "Machine Learning Approaches in Cybersecurity," no. February, pp. 345–357, 2022, doi: 10.1007/978-981-16-6460-1_26.

[41] J. Bharadiya, "Machine Learning in Cybersecurity: Techniques and Challenges," *Eur. J. Technol.*, vol. 7, no. 2, pp. 1–14, 2023, doi: 10.47672/ejt.1486.

[42] P. Shamsolmoali and M. Zareapoor, “Statistical-based filtering system against DDOS attacks in cloud computing,” *Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014*, pp. 1234–1239, 2014, doi: 10.1109/ICACCI.2014.6968282.

[43] P. Xiao, W. Qu, H. Qi, and Z. Li, “Detecting DDoS attacks against data center with correlation analysis,” *Comput. Commun.*, vol. 67, pp. 66–74, 2015, doi: 10.1016/j.comcom.2015.06.012.

[44] Vrizlynn L. L. Thing, “IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach,” *IEEE Wirel. Commun. Netw. Conf.*, 2017.

[45] G. S. Kushwah and S. T. Ali, “Detecting DDoS attacks in cloud computing using ANN and black hole optimization,” *2nd Int. Conf. Telecommun. Networks, TEL-NET 2017*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/TEL-NET.2017.8343555.

[46] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, “Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods,” *IEEE Access*, vol. 7, no. 1, pp. 51691–51713, 2019, doi: 10.1109/ACCESS.2019.2908998.

[47] Zheng Bojun1, Ma Tongtong2, Liu Boxuan, " An image encryption system based on random matrix interpolation followed by iterative generation of sequences", Mustansiriyah Journal of Pure and Applied Sciences, Vol. 2, No.2 (2024) 96–111

[48] I. Ullah and Q. H. Mahmoud, “A two-level flow-based anomalous activity detection system for IoT networks,” *Electron.*, vol. 9, no. 3, 2020, doi: 10.3390/electronics9030530.

[49] J. Lee, J. Kim, I. Kim, and K. Han, “Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles,” *IEEE Access*, vol. 7, pp. 165607–165626, 2019, doi: 10.1109/ACCESS.2019.2953095.