Received: 10 May 2024, Revised: 17 June 2024, Accepted: 18 June 2024, Online: 13 July 2024

DOI: https://doi.org/10.55708/js0307002

A Thorough Examination of the Importance of Machine Learning and Deep Learning Methodologies in the Realm of Cybersecurity: An Exhaustive Analysis

Ramsha Khalid *[1,2] **, Muhammad Naqi Raza** [1]

[1] Electrical Engineering Technology, University of Sialkot, Sialkot, 51310, Pakistan

[2] Electrical Engineering, University of Lahore, Lahore, 53720, Pakistan

*Corresponding author: Ramsha Khalid, University of Sialkot, Sialkot, Email: ramshakhalid2404@gmail.com

ABSTRACT: In today's digital age, individuals extensively engage with virtual environments hosting a plethora of public and private services alongside social platforms. As a consequence, safeguarding these environments from potential cyber threats such as data breaches and system disruptions becomes paramount. Cybersecurity encompasses a suite of technical, organizational, and managerial measures aimed at thwarting unauthorized access or misuse of electronic information and communication systems. Its objectives include ensuring operational continuity, safeguarding the confidentiality and integrity of sensitive data, and shielding consumers from various forms of cyber intrusions. This paper delves into the realm of cybersecurity practices devised to fortify computer systems against diverse threats including hacking and data breaches. It examines the pivotal role of artificial intelligence within this domain, offering insights into the utilization of machine learning and deep learning techniques. Moreover, it synthesizes key findings from relevant literature exploring the efficacy and impact of these advanced methodologies in cybersecurity. Findings underscore the substantial contributions of machine learning and deep learning techniques in fortifying computer systems against unauthorized access and mitigating the risks posed by malicious software. These methodologies facilitate proactive measures by predicting and comprehending the behavioral patterns and traffic associated with potential cyber threats.

KEYWORDS: Cybersecurity, Cyber attackers, Artificial intelligence, Machine learning, Deep learning, Communication systems, Unauthorized entry

1. Introduction

The Internet has transformed various facets of contemporary life, creating a global village where knowledge exchange and cultural interactions flourish. Networks form the backbone of this digital landscape, connecting devices such as computers and mobile phones. Their significance lies in enabling access to the Internet; without it, these devices lose much of their functionality. Through networks, data, information, and applications flow seamlessly via physical cables and wireless radio waves. Protecting personal data, crucial for transactions conducted over networks, is paramount amidst the looming threat of hackers aiming for identity theft or fraudulent activities [1]. The COVID-19 pandemic catalyzed a shift towards digital transactions with minimal physical contact to mitigate virus transmission. This transition propelled widespread adoption of electronic transactions by institutions and businesses, highlighting their efficiency and accessibility benefits for consumers. Simultaneously, online shopping platforms, including those on social media like Facebook, witnessed increased activity, facilitating the sale and distribution of goods [2,3]. Moreover, educational institutions transitioned to online platforms for delivering education and training, reflecting a growing acceptance of digital learning modalities. Similarly, remote work gained traction as a viable option for both public and private sector organizations, facilitated by the widespread availability of Internet connectivity [4,5].

As remote work liberates employees from fixed locations, the sharing of online workspaces necessitates information security specialists to evaluate the associated business risks and prevent unauthorized access or hacking attempts from external parties [6,7]. Despite the implementation of sophisticated technical security measures by organizations to combat cyber threats, the human element remains a critical consideration, as employees' skills often constitute the weakest link in the security chain. It is imperative for employees to be vigilant against potential hacking or malicious software threats that may compromise their data unbeknownst to them. In addition to conducting awareness-raising activities such as training sessions and workshops for employees lacking expertise in cybersecurity, organizations must also enforce a range of technical safeguards. Practices posing threats to information security include leaving computers unlocked while unattended, abandoning devices in public settings, and disregarding company policies regarding password security. Consequently, there is a pressing need for further investigation into the risks associated with remote work.

1.1. Artificial Intelligence

Artificial intelligence techniques have emerged as some of the most advanced and invaluable tools in various fields, including cybersecurity and information security [8,9]. AI encompasses the capability of machines, electronic devices, software, applications, and gaming consoles to mimic human brain functions, such as awareness, memory, and data utilization, in decision-making processes [10]. Equipped with electronic brains, AI-enabled devices can analyze data and perform required operations, leveraging insights garnered from experimental data. The term "cybersecurity" has gained prominence in response to the widespread adoption and accessibility of Internet networks, particularly with the advent of 5G technology [11]. The proliferation of electronic crimes targeting data, information, and applications on computers and electronic devices underscores the imperative for robust security measures. Consequently, companies are increasingly turning to AI-based techniques to forecast cybercrime activities, preempt attacks, and thwart unauthorized intrusions into computer systems. Compared to human specialists, AI techniques offer superior efficacy in scrutinizing network users for authorization, thereby enhancing security protocols [12,13]. Moreover, their capacity for rapid learning, retention, and task execution translates into significant time and resource savings for experts. Notably, AI techniques excel in recognizing repetitive patterns, a feature invaluable in cybersecurity for identifying and analyzing user behaviors and predicting anomalous activities indicative of malware infiltration [14,15].

This paper makes a substantial contribution b elucidating the pivotal role of machine learning and deep learning techniques in cybersecurity. It showcases their efficacy in mitigating intrusions and attacks on computer systems while elucidating their diverse applications within the cyber domain. Additionally, the paper provides a succinct overview of seminal studies leveraging these techniques in cybersecurity, scrutinizing their findings and elucidating their impact on decision-making processes. The data utilized in this paper are sourced from reputable news outlets and scholarly literature, streamlining the research process for cybersecurity scholars and practitioners.

The subsequent sections of this paper are structured as follows: Section 2 provides an examination of prevailing cybersecurity practices and the attendant challenges confronting computer systems. In Section 3, an overview of prominent datasets employed in attack and intrusion detection is presented. Sections 4 and 5 delve into the importance of machine learning and deep learning methodologies in cybersecurity, along with a comprehensive review of key literature utilizing these techniques. Finally, Section 6 offers concluding remarks.

2. Cybersecurity Practices

In recent years, the electronics and technology industry has experienced significant growth, becoming an integral part of daily life for individuals, indispensable for the fulfillment of business endeavors and projects. The functionality of modern devices relies on a suite of applications designed to serve human needs, necessitating comprehensive protective measures to safeguard against intrusions, hacking, attacks, and unauthorized access [16,17]. Concerns regarding hacking and data theft loom large for numerous companies and institutions. As organizations across diverse sectors increasingly acknowledge the paramount importance of their data, attention to cybersecurity has surged. This encompasses various facets, including measures to secure communication systems, data, and raw information, as well as virtual and physical components associated with operating systems. Secure applications, accessible only to authorized personnel, are vital elements within this framework [18–20]. Described as a combination of tools and practices, cybersecurity serves to defend computer systems' contents and thwart the infiltration of malicious software [21]. Table 1 provides a comprehensive summary of the various types of cybersecurity and their roles in safeguarding computer systems. Fundamental to cybersecurity are three key features: confidentiality, ensuring that unauthorized individuals cannot access or manipulate data within a computer system; integrity, preventing unauthorized modification or deletion of data; and availability, ensuring that data, information, and communications reach intended recipients without interception or decryption by unauthorized parties. Regardless of location, cyberattacks pose significant risks

to organizations, their employees, and their clientele, potentially resulting in profound consequences. Thus, it is imperative for employees to possess awareness of their organizations' cybersecurity protocols and adopt practices to mitigate associated risks. Table 2 illustrates significant instances of cyberattacks.

Table 1: Types of Cybersecurity and Their Functions

Cybersecurity Category	Functions
Application Security	Execute intricate codes to safeguard and encrypt data effectively [22]
Information Security	Ensure data protection from unauthorized access and alterations [23]
Infrastructure Security	Secure critical infrastructures such as power networks and data centers, ensuring absence of vulnerabilities [24]
Network Security	Protect networks from intrusions using tools like remote access management, two-factor authentication (2FA), and robust firewalls [25]
User Education	Provide valuable training sessions and conferences for employees and cybersecurity professionals [26]

Table 2: Types of Cybersecurity Attacks

Type	Description
Malware	A collection of malicious applications designed to damage systems and steal data [27]
Ransomware	Malicious software that encrypts data, disables systems, and restricts authorized user access [28]
Phishing	A common form of social engineering wherein individuals are manipulated into divulging sensitive information, posing significant security risks [29]
DDoS	Denial-of-Service attacks that disrupt systems, preventing user access to network resources, and inflicting financial or reputational harm on organizations [30]
SQL Injection	Exploits web security vulnerabilities to access, steal, modify, or delete data from websites, leading to system dysfunction [31]
Zero-Day Exploit	Newly discovered security vulnerabilities exploited by hackers to target computer systems, often leaving administrators with insufficient time to address the issue [32]
DNS Tunnelling	A sophisticated attack technique involving the encoding of system data and applications, challenging to detect [33]
XSS Attacks	Injection of malware into trusted websites, camouflaged as benign browser scripts [34]

The initial instance of malicious software, Creeper, surfaced in the 1970s with the capacity to destruct computer data. Upon infection, affected computers displayed a notable message on their screens: "I'm a creeper, catch me if you can!". In response to this emerging threat, the inaugural antivirus program, known as Reaper, was developed.

In 1903, Nevil Maskelyne made history as the first documented hacker by intercepting the inaugural wireless telegraph transmission, thereby revealing vulnerabilities inherent in Marconi's system. Concurrently, John Draper emerged as the pioneering cybercriminal, having discovered that the whistle included in Cap'n Crunch cereal boxes emitted a tone capable of deceiving telephone exchange signals, enabling him to place unauthorized free calls..

2.1. Cybersecurity Data Science

Data science encompasses the analysis of diverse data domains, ranging from life sciences to consumer behavior and cybersecurity. It plays a pivotal role in shaping the future of systems and cybersecurity fields, given its reliance on comprehensive data sets. Detecting cyber threats hinges on the meticulous analysis of security data, including files, records, and user activities within a network. Cybersecurity professionals leverage various techniques such as file hashes and custom rules, such as signatures or heuristics, to trace the origins of incoming data streams. While these manual methods offer unique advantages, they demand significant efforts to stay abreast of evolving threats and breaches.

Figure 1 illustrates the transformation of big data into actionable decisions, while Table 3 delineates various types of cybersecurity attacks. Data science endeavors to revolutionize information technology by leveraging machine learning and deep learning techniques to identify and address system vulnerabilities through feature extraction and pattern recognition from training data. Over the past decade, cybersecurity has increasingly relied on data science and artificial intelligence due to their capability to convert raw data into actionable insights and fortify system security.

In essence, data science offers an efficient approach to decision-making through tasks such as data engineering for data accumulation and analysis, data volume reduction through critical data filtering, discovery of unique patterns and data learning techniques, development of innovative data-driven security models, knowledge generation for mitigating false alerts, and optimization of system resources.

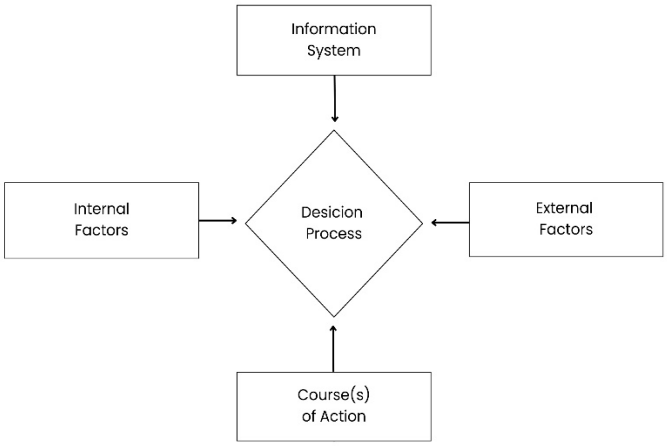

Figure 1: Representation of the process of data analysis and decision-making

Table 3: Prominent datasets utilized in cybersecurity research.

Dataset	Description
DARPA	Contains intrusion detection data, including LLDOS-1.0 and LLDOS-2.0.2, depicting connections between source and destination IP addresses, categorized by MIT Lincoln Laboratory for evaluating attacks and intrusion detection [35].
CAIDA	Encompasses distributed denial of service (DDoS) attack traffic and regular traffic traces, including unspecified traffic from a 2007 DDoS attack, facilitating evaluation of machine-learning-based detection models for identifying DoS activity on the Internet [36].
CTU-13	Comprises botnet traffic captured by a Czech university in 2011, featuring real botnet traffic mixed with normal and background traffic across 13 scenarios, suitable for data-based malware analysis employing machine learning techniques [37].
KDD'99 Cup	Widely used dataset since 1999 with 41 features for evaluating anomaly detection, categorizing attacks into probing, remote-to-local (R2L), user-to-remote (U2R), and DoS, suitable for assessing machine-learning-based attack detection models [38].
NSL-KDD	Revised version of KDD'99 Cup dataset, eliminating redundant records and addressing inherent issues to avoid bias towards frequent records [39].
MAWI	Dataset aiding researchers in anomaly detection, sourced from Japanese network research institutions, featuring traffic deviation labels in the MAWI archive, revised daily to include all traffic from applications and malware [40].
ISCX'12	Produced by Canadian Institute for Cybersecurity, containing 19 features for machine-learning-based attack detection and network penetration models, used in real-time with expert input to prevent system destruction and data theft [41].
Bot-IoT	Simulated Internet of Things environment dataset from UNSW Canberra Cyber Range Lab, featuring reliable traffic and various attack types, including DDoS, DoS, OS and service scan, keylogging, and data exfiltration, organized by protocol [42].
ISOT'10	Mix of malicious and non-malicious data traffic dataset from University of Victoria's ISOT research, utilized for evaluating models, machine-learning-based classification, and attack and penetration localization [43].
UNSW-NB15	Created using IXIA PerfectStorm tool in UNSW Canberra Cyber Range Lab, comprising contemporary synthetic attack activities and behaviors, with 49 features and 9 attack types, generated from TCPDUMP, ARGUS, and Bro-IDS tools [44].

2.2. Machine Learning in Cybersecurity

Electronic devices are experiencing rapid advancements, attracting a substantial following across various domains. However, the extensive communication and data exchange among these devices pose significant risks, notably concerning data breaches. Scholars advocate for leveraging machine learning techniques to

mitigate electronic threats, although these methods are still in developmental stages. Cyber threats are dynamic, necessitating adaptive solutions. Machine learning stands out as a potent tool due to its adaptability and learning capabilities. While effective in detecting and thwarting known malware attacks, machine learning faces challenges against novel threats. Operating within the realm of artificial intelligence, machine learning employs statistical operations to analyze data, extract insights, and aid decision- making. Its core objective is to enable computers to learn from expert-provided data [45–47]. Machine learning techniques encompass various rules and methodologies aimed at identifying or predicting novel data patterns or behaviors. These techniques find application in cybersecurity and can be categorized into supervised and unsupervised methods. Despite the substantial adoption of machine learning in cybersecurity, these tools remain imperfect, demanding significant human oversight, and necessitating continuous retraining of algorithms due to the inability to fully automate data processes [48,49]. This segment explores the functionality of machine learning techniques and their integration into cybersecurity practices. Figure 2 elucidates the operational framework of these techniques in detecting anomalies within a system.

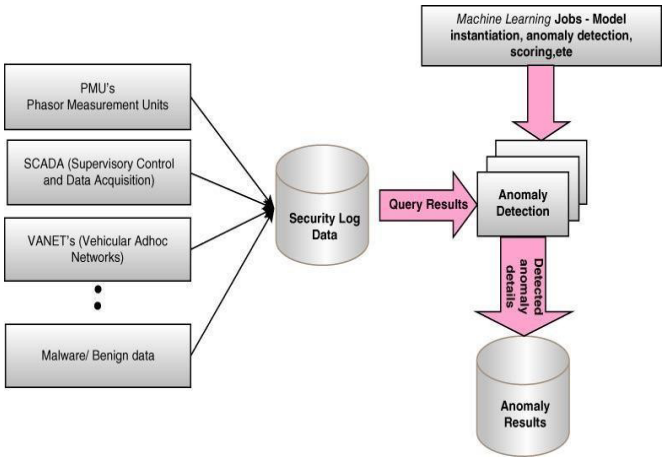

Figure 2: Utilizing machine learning techniques for anomaly detection [54].

2.2.1. *Supervised Learning*

Supervised learning functions methodically by establishing precise objectives and achieving them through a defined set of inputs [50]. Widely employed across various domains, supervised learning techniques offer straightforward implementation and monitoring. They are typically classified into classification and regression methods, which respectively categorize security data or anticipate specific security issues to be addressed in the future. The failure of an organization to avert an anticipated attack on its computer system can have far-reaching consequences, leading to substantial financial losses and necessitating a laborious recovery process in Figure 3. Consequently, the utilization of machine learning techniques in cybersecurity is advocated to bolster data protection across all sectors and safeguard the data of both organizations and their users. Notable supervised learning techniques in classification include logistic regression, decision trees, support vector machines, k-nearest neighbors, and naive Bayes. These techniques are also applied in prediction tasks owing to their capacity to construct data-driven predictive models. For instance, the activities of users within a network, whether in a public or private institution, can be forecasted by continually tracking their actions, gathering relevant data, and discerning between processes initiated by human users and those generated by bots impacting the network. Meanwhile, prominent regression techniques in supervised learning, such as linear regression and support vector regression, are utilized to identify underlying causes of significant cybercrimes that profoundly affect individuals' lives and develop corresponding solutions. The distinction between classification and regression techniques lies in their respective outcomes: classification yields categorical or discrete results/effects, whereas regression produces numeric or continuous outputs/effects.

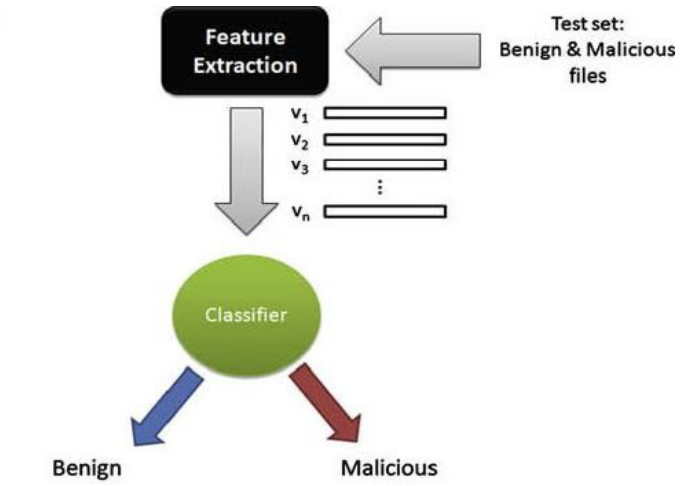

Figure 3: Utilizing machine learning techniques to classify unidentified datasets as either malicious or benign.

2.2.2. *Unsupervised Learning*

The primary objective of unsupervised learning techniques is to unveil patterns, structures, or insights from unlabelled data. However, within cybersecurity, malware often evade detection by dynamically altering their operations [51]. Clustering techniques, including k-means, k- medoids, and single linkage, constitute unsupervised learning methods aimed at uncovering hidden and intricate attack patterns and structures within large datasets. These techniques play a pivotal role in identifying and notifying users or developers about anomalies within systems, breaches of privacy policies, and unauthorized data accesses. Engineering tasks associated with these technologies, such as optimizing dataset features or extracting pertinent features related to specific security issues, are deemed essential for

conducting further analyses, irrespective of dataset scale. Moreover, security features are prioritized based on their significance. Additional methods like linear discriminant analysis, principal component analysis, non-negative matrix factorization, and Pearson correlation analysis contribute to addressing cybersecurity threats and uncovering clandestine programs using machine learning to preempt attacks and data breaches. In expert systems, rules are manually defined and implemented by a knowledge engineer in collaboration with a cybersecurity expert. Association rules learning aims to identify existing rules or relationships among datasets to extract relevant security attributes. Correlation analysis assesses the strength of relationships among datasets. Data mining techniques are categorized into frequent pattern-based, logic-based, and tree-based methods. Techniques such as AIS, Apriori, Apriori-TID, Apriori-Hybrid, FP-Tree, RARM, and Eclat are employed to formulate association rules capable of detecting intrusion and data theft issues. Table 4 enumerates the ten most impactful studies concerning the application of machine learning techniques in identifying attacks on operating systems.

Table 4: Scholarly works exploring the application of machine learning methodologies in identifying attacks and malicious software.

Article	Purpose	Techniques	Most Suitable Effect
[52]	Detect distributed denial- of-service (DDoS) attacksand malicious data.	MLP, K-NN, SVM, FL, ED, and MNB	The most suitable classification method is the MLP technique, achieving an F1-score of over 98% for emulated traffic and over 99% for real traffic.
[53]	Develop an intrusion detection system employing an efficient and reliable classifier.	SVM	The authors achieve a high accuracy of 98.62%,deemed excellent in intrusion detection.
[54]	Design a knowledge-based alert verification strategy with an intelligent filter to eliminate unwanted alarms.	KNN	KNN demonstrates the highest performance accuracy of 93.2% and the most robust F-measure of 91.8%.
[55]	Conduct experiments on five million Android applications to detect malicious software in the Android OS by recognizing features.	DL, FFC, Y-MLP, and DT	These methods achieve apeak performance accuracy of over 98% in identifying malicious software.
[56]	Detect ransomware tools (RANDS) operating within Windows environments through three stages (ransomware analysis, learning, and detection).	NB and DT	These methods attain an average classification accuracy of 96.27% in categorizing ransomware, with a 1.32% average real-time execution error.
[57]	Utilize a dataset of 300,000 attributes to predict and detect ransomware.	SVM	The technique reports an accuracy exceeding 88% in ransomware classification.
[58]	Monitor systems and detect intrusions by analyzing incoming data activities of servers and identifying malicious software.	DT with binary split	This technique achieves an impressive attack detection accuracy of over 99%.
[59]	Enhance the performance of the random forest strategy to detect misuse, anomaly, and hybrid-	New systematic frameworks of RF	These frameworks achieve a high detection rate in identifying and reporting anomalies.

	network-based intrusion detection systems (IDSs).		
[60]	Detect denial-of-service (DOS) attacks in software-defined networks (SDNs) and address cybersecurity management in SDN architectures.	KNN, RF, SVM, and ANN	These methods achieve an accuracy exceeding 98% in detecting DOS attacks.
[61]	Detect intrusions and identify malicious data through data mining techniques.	FCM, ANN, and SVM	These methods achieve a peak accuracy of 98.99% in detecting remote to-local (R2L) attacks.

However, machine learning techniques are not without their constraints. For instance, they are incapable of identifying attacks that have not been previously encountered. Furthermore, the detection of behavioral patterns and anomalies may result in false positives if the behavioral restriction policy is overly broad. Conversely, implementing a stricter policy could diminish the effectiveness of these techniques. The selection of appropriate datasets is also crucial during the training phase of machine learning techniques in cybersecurity endeavors. Without proper training, these techniques may fail to deliver the anticipated results. When cyber adversaries become aware of a security system relying solely on a single defense technology, they may devise strategies to bypass such systems, such as through hacking. Nonetheless, a robust cybersecurity framework grounded in machine learning can leverage multiple complementary techniques.

2.3. Deep Learning in Cybersecurity

To address the intricate challenges in cybersecurity, various methodologies are employed based on specific criteria such as data volume, issue type, sensitivity, and decision tolerance. Deep learning techniques, leveraging parallel processing, prove highly effective in handling large- scale data and entail complex procedures [62–64]. This section critically examines the literature implementing deep learning methodologies for intrusion detection, attack mitigation, and malware identification. These studies are succinctly outlined in Table 5. Deep learning architectures are not configured solely on local platforms; rather, they are deployed on server- based systems to ensure data integrity, confidentiality, and reliability, while also safeguarding against unauthorized access. The development of a robust deep learning model in cybersecurity involves two primary stages. Initially, the data transfer area is encrypted within the local environment before transmitting to the server. Subsequently, upon reaching the server, these encrypted data are processed, classified, and identified. For example, in character recognition from images, the first stage encompasses character encoding and transmission, while the second stage involves processing the received data and detecting any potential man-in-the- middle attacks between the server and local system, crucial for accurate data classification. This approach ensures secure information transmission to users, preventing unauthorized access to the system.

In networked environments, ensuring appropriate security measures and robust data preservation, storage, and transmission mechanisms are imperative responsibilities of the companies managing these systems. Breaches in networked systems vary depending on network activity and scale, with larger and more active networks encountering higher volumes of data requiring processing. To efficiently handle such data influx, parallel processing and deep learning techniques are favored for their speed and accuracy [65–67]. Deep learning methodologies have emerged as effective tools for detecting malware, given their capability to analyze various characteristics of malicious programs that can disrupt system operations by altering data. Numerous researchers have employed convolutional neural networks for classifying data, extracting essential features, and isolating genetic sequences indicative of malicious applications, thereby facilitating network training. Moreover, deep learning techniques are instrumental in identifying biological attributes such as personal identification numbers (PINs) and passwords, recognizing user voices or images, and analyzing behavior- based licenses. At this stage, techniques derived from recurrent neural networks (RNNs), including gated recurrent units and long short-term memory, are often deployed.

Device security stands as a pivotal concern within the realm of cybersecurity, wherein heightened security measures necessitate increased interactions between humans and electronic environments. Deep learning techniques play a crucial role in safeguarding data, systems, and applications. Renowned for their exceptional performance in processing 2D and 3D media data as well as vast datasets, these techniques are

extensively employed in image and video processing. In the cybersecurity domain, deep learning endeavors to discern the suitability of received data for supervised or unsupervised techniques and to evaluate the influence of prior knowledge on subsequent insights. Moreover, deep learning assesses system performance in addressing problems across both one- and multi-dimensional examples. Scholars are actively exploring deep learning methodologies to devise solutions for numerous cybersecurity challenges [68–70].

Table 5: Scholarly works employing deep learning methodologies for the detection of attacks and malicious software.

Article	Purpose	Technique use	Most Suitable Effect
[71]	Protect autonomous vehicle systems from attacks and ensure control.	CNN and CNN-LSTM	Achieves a remarkably high accuracy exceeding 97% in identifying attack messages and preventing their display on vehicle screens.
[72]	Real-time intrusion detection in vehicular data encompassing cyber and physical processes.	LR, SVM, RF, DT, MLP, and RNN	RNN exhibits the best accuracy of 79.3% in detecting malware, denial-of-service (DoS) attacks, and command injections.
[73]	Predict software vulnerabilities and identify accessible features at an early stage.	ExBERT framework	ExBERT framework reveals over 46,000 vulnerabilities with a prediction accuracy surpassing 91%.
[74]	Analyze and detect attacks using URLs on edge devices, safeguarding data in cloud-Internet of Things (IoT) systems.	Multiple concurrent deep models	These models achieve a high accuracy of over 99% in detecting normal requests.
[75]	Develop an intrusion detection application and protect computer systems.	MLP and PID	MLP and PID attain an accuracy of 98.96% in intrusion detection and understanding attack types.
[76]	Detect intrusions and analyze network anomalies.	K-NN and DNN	DNN achieves over 92% accuracy in intrusion detection.
[77]	Establish an intrusion detection approach for cyber-attack security and classification.	RNN	RNN achieves the highest accuracy of 98.27%.
[78]	Enhance simulation training methods to detect anomaly intrusion via the Internet.	RBM and DBM	RBM and DBM demonstrate an exceptional accuracy of 97.9% in detecting anomaly intrusions.
[79]	Identify malicious programs in multi-cloud healthcare systems using the MUSE model.	DHSNN	DHSNN achieves excellent training and testing accuracies ranging from 95% to 100% in detecting new attacks on dataflows.
[80]	Classify a traffic detection system and network fault identification or intrusion detection system.	CNN	CNN reports an efficacy of over 99%.

3. Conclusion and Future Work

Artificial intelligence stands as a cornerstone of the Fourth Industrial Revolution, poised to continue its profound impact on society due to its manifold benefits. However, to strike a harmonious balance between technological advancement and fundamental human values, the nexus between artificial intelligence and cybersecurity requires thorough exploration. It is imperative to harness modern technologies within virtual environments and social networking platforms to safeguard user privacy and information. The evolution of artificial intelligence capabilities must parallel the emergence of novel applications, fostering digital collaboration among nations and leveraging the integration of digital technologies into physical settings. Facilitating unrestricted access to data for researchers, while upholding user privacy, is essential for training artificial intelligence algorithms and conducting data analysis on a broader scale. Increased financial and ethical investments in machine learning and deep learning are vital to fortify the privacy of social media users and mitigate data breaches. Continuous training for cybersecurity professionals on cutting-edge technologies, hacker tactics, and malware behavior is imperative. Furthermore, stringent penalties and fines should be enforced for the misuse of artificial intelligence techniques and unauthorized privacy breaches. Future research endeavors should focus on implementing these techniques for predictive and classification purposes in cybersecurity, thus optimizing their efficacy.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] N. Bhalaji, "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks," *Journal of IoT in Social, Mobile, Analytics, and Cloud*, vol. 2, no. 2, 106–117, 2020, doi:10.36548/jismac.2020.2.004.

[2] J. Budd, B.S. Miller, E.M. Manning, V. Lampos, M.Z. et al., "Digital technologies in the public-health response to COVID-19," *Nature Medicine*, vol. 26, 1183–1192, 2020, doi:10.1038/s41591-020-1011-4.

[3] K. Leung, J.T. Wu, G.M. Leung, "Real-time tracking and prediction of COVID-19 infection using digital proxies of population mobility and mixing," *Nature Communications*, vol. 12, no. 1501, 1–8, 2021, doi:10.1038/s41467-021-21776-2.

[4] S. Shrestha, S. Haque, S. Dawadi, R.A. Giri, "Preparations for and practices of online education during the Covid-19 pandemic: A study of Bangladesh and Nepal," *Education and Information Technologies*, vol. 27, 243–265, 2021, doi:10.1007/s10639-021-10659-0.

[5] M. Ssenyonga, "Imperatives for post COVID-19 recovery of Indonesia's education, labor, and SME sectors," *Cogent Economics & Finance*, vol. 9, no. 1, 1–51, 2021, doi:10.1080/23322039.2021.1911439.

[6] H. Saleous, M. Ismail, S.H. AlDaajeh, N. Madathil, S. Alrabaee, "COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities," *Digital Communications and Networks*, vol. In press, , 2022, doi:10.1016/j.dcan.2022.06.005.

[7] H.S. Lallie, L.A. Shepherd, J.R.C. Nurse, A. Erola, G.E. et al., "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, 102248, 2021, doi:10.1016/j.cose.2021.102248.

[8] J. Li, "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, 1462–1474, 2019, doi:10.1631/FITEE.1800573.

[9] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, F.Z. et al., "Artificial intelligence in cyber security: research advances, challenges, and opportunities," *Artificial Intelligence Review*, vol. 55, 1029–1053, 2021, doi:10.1007/s10462-021-09976-0.

[10] M.M. Mijwil, "Implementation of Machine Learning Techniques for the Classification of Lung X-Ray Images Used to Detect COVID-19 in Humans," *Iraqi Journal of Science*, vol. 62, no. 6, 2099–2109, 2021, doi:10.24996/ijs.2021.62.6.35.

[11] J. Cáceres-Hidalgo, D. Avila-Pesantez, "Cybersecurity Study in 5G Network Slicing Technology: A Systematic Mapping Review," in *Proceedings of IEEE Fifth Ecuador Technical Chapters Meeting*, IEEE, Cuenca, Ecuador: 1–6, 2021, doi:10.1109/ETCM53643.2021.9590742.

[12] T. Ghosh, H. Al Banna, S. Rahman, S. Kaiser, M.M. et al., "Artificial intelligence and internet of things in screening and management of autism spectrum disorder," *Sustainable Cities and Society*, vol. 74, 103189, 2021, doi:10.1016/j.scs.2021.103189.

[13] A. Adadi, M. Lahmer, S. Nasiri, "Artificial Intelligence and COVID-19: A Systematic umbrella review and roads ahead," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, 5898–5920, 2022, doi:10.1016/j.jksuci.2021.07.010.

[14] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N.A. et al., "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electronics*, vol. 11, no. 2, 1–27, 2022, doi:10.3390/electronics11020198.

[15] I.F. Kilincer, F. Ertam, A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, 107840, 2021, doi:10.1016/j.comnet.2021.107840.

[16] S. Kuipers, M. Schonheit, "Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises," *Corporate Reputation Review*, vol. 25, 176–197, 2021, doi:10.1057/s41299-021-00121-9.

[17] N. Rawindaran, A. Jayal, E. Prakash, C. Hewage, "Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME)," *Future Internet*, vol. 13, no. 8, 1–36, 2021, doi:10.3390/fi13080186.

[18] F. Quayyum, D.S. Cruzes, L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction*, vol. 30, 100343, 2021, doi:10.1016/j.ijcci.2021.100343.

[19] P. Formosa, M. Wilson, D. Richards, "A principlist framework for cybersecurity ethics," *Computers & Security*, vol. 109, 102382, 2021, doi:10.1016/j.cose.2021.102382.

[20] I.H. Sarker, H. Furhad, R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," *SN Computer Science*, vol. 2, no. 173, 2021, doi:10.1007/s42979-021-00557-0.

[21] E. Fosch-Villaronga, T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Computer Law & Security Review*, vol. 41, 105528, 2021, doi:10.1016/j.clsr.2021.105528.

[22] P. Sharma, S. Jain, S. Gupta, V. Chamola, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Networks*, vol. 123, 102685, 2021, doi:10.1016/j.adhoc.2021.102685.

[23] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M.S. et al., "Data hiding technique in steganography for information security using number theory," *Journal of Information Science*, vol. 45, no. 6, 767–778, 2018, doi:10.1177/0165551518816303.

[24] G. Hale, C. Bartlett, "Managing the Regulatory Tangle: Critical Infrastructure Security and Distributed Governance in Alberta's Major Traded Sectors," *Journal of Borderlands Studies*, vol. 34, no. 2, 257–279, 2018, doi:10.1080/08865655.2017.1367710.

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

[26] D.G. Broo, U. Boman, M. Törngren, "Cyber-physical systems research and education in 2030: Scenarios and strategies," *Journal of Industrial Information Integration*, vol. 21, 100192, 2021, doi:10.1016/j.jii.2020.100192.

[27] M.M. Mijwil, "Malware Detection in Android OS Using Machine Learning Techniques," *Data Science and Applications*, vol. 3, no. 2, 5–9, 2020.

[28] U. Urooj, B.A.S. Al-rimy, A. Zainal, F.A. Ghaleb, M.A. Rassam, "Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions," *Applied Sciences*, vol. 12, no. 1, 1–45, 2021, doi:10.3390/app12010172.

[29] A.F. AL-Otaibi, E.S. Alsuwat, "A Study on Social Engineering Attacks: Phishing Attack," *International Journal of Recent Advances in Multidisciplinary Research*, vol. 7, no. 11, 6374–6379, 2020.

[30] A. Narote, V. Zutshi, A. Potdar, R. Vichare, "Detection of DDoS Attacks using Concepts of Machine Learning," *International Journal for Research in Applied Science & Engineering Technology*, vol. 10, no. VI, 390–403, 2022.

[31] N. Bedeković, L. Havaš, T. Horvat, D. Crčić, "The Importance of Developing Preventive Techniques for SQL Injection Attacks," *Tehnički Glasnik*, vol. 16, no. 4, 523–529, 2022, doi:10.31803/tg-20211203090618.

[32] U.K. Singh, C. Joshi, D. Kanellopoulos, "A framework for zero-day vulnerabilities detection and prioritization," *Journal of Information Security and Applications*, vol. 46, 164–172, 2019, doi:10.1016/j.jisa.2019.03.011.

[33] Y. Wang, A. Zhou, S. Liao, R. Zheng, R. Hu, L. Zhang, "A comprehensive survey on DNS tunnel detection," *Computer Networks*, vol. 179, 108322, 2021, doi:10.1016/j.comnet.2021.108322.

[34] Y. Zhou, P. Wang, "An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence," *Computers & Security*, vol. 82, 261–269, 2019, doi:10.1016/j.cose.2018.12.016.

[35] J. He, C. Chang, P. He, M.S. Pathan, "Network Forensics Method Based on Evidence Graph and Vulnerability Reasoning," *Future Internet*, vol. 8, no. 4, 1–18, 2016, doi:10.3390/fi8040054.

[36] M.P. Singh, A. Bhandari, "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges," *Computer Communications*, vol. 15, 509–527, 2020, doi:10.1016/j.comcom.2020.02.085.

[37] J.L.G. Torres, C.A. Catania, E. Veas, "Active learning approach to label network traffic datasets," *Journal of Information Security and Applications*, vol. 49, 102388, 2019, doi:10.1016/j.jisa.2019.102388.

[38] S. Choudhary, N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," *Procedia Computer Science*, vol. 167, 1561–1573, 2020, doi:10.1016/j.procs.2020.03.367.

[39] L. Dhanabal, S.P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 6, 446–452, 2015.

[40] B. Bouyeddou, F. Harrou, B. Kadri, Y. Sun, "Detecting network cyber-attacks using an integrated statistical approach," *Cluster Computing*, vol. 24, 1435–1453, 2020, doi:10.1007/s10586-020-03203-1.

[41] M. Idhammad, K. Afdel, M. Belouch, "Semi-supervised machine learning approach for DDoS detection," *Applied Intelligence*, vol. 48, 3193–3208, 2018, doi:10.1007/s10489-018-1141-2.

[42] N. Koroniotis, N. Moustafa, E. Sitnikova, B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, 779–796, 2019, doi:10.1016/j.future.2019.05.041.

[43] I.H. Sarker, "Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective," *SN Computer Science*, vol. 2, no. 154, 1–16, 2021, doi:10.1007/s42979-021-00535-6.

[44] S.M. Kasongo, Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *Journal of Big Data*, vol. 7, no. 105, 1–20, 2020, doi:10.1186/s40537-020-00379-6.

[45] R.T. S., R. Sathya, "Ensemble Machine Learning Techniques for Attack Prediction in NIDS Environment," *Iraqi Journal For Computer Science and Mathematics*, vol. 3, no. 2, 78–82, 2022, doi:10.52866/ijcsm.2022.02.01.008.

[46] Y. Niu, A. Korneev, "Identification Method of Power Internet Attack Information Based on Machine Learning," *Iraqi Journal For Computer Science and Mathematics*, vol. 3, no. 2, 1–7, 2022, doi:10.52866/ijcsm.2022.02.01.001.

[47] M.M. Mijwil, E.A. Al-Zubaidi, "Medical Image Classification for Coronavirus Disease (COVID-19) Using Convolutional Neural Networks," *Iraqi Journal of Science*, vol. 62, no. 8, 2740–2747, 2021, doi:10.24996/ijs.2021.62.8.27.

[48] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, M. Portmann, "Feature extraction for machine learning-based intrusion detection in IoT networks," *Digital Communications and Networks*, vol. In press, , 2022, doi:10.1016/j.dcan.2022.08.012.

[49] M.A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, M. Samaka, "SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach," *Future Internet*, vol. 10, no. 8, 1–15, 2018, doi:10.3390/fi10080076.

[50] K. Aggarwal, M.M. Mijwil, Sonia, A.H. Al-Mistarehi, S. Alomari, M. Gök, A.M. Alaabdin, S.H. Abdulrhman, "Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, 115–123, 2022, doi:10.52866/ijcsm.2022.01.01.013.

[51] L.F. Maimó, A.H. Celdrán, A.L.P. Gómez, F.J.G. Clemente, J. Weimer, I. Lee, "Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments," *Sensors*, vol. 19, no. 5, 1–31, 2019, doi:10.3390/s19051114.

[52] V.M. Rios, P.R.M. Inácio, D. Magoni, M.M. Freire, "Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms," *Computer Networks*, vol. 186, 107792, 2021, doi:10.1016/j.comnet.2020.107792.

[53] Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, K. Dai, "An efficient intrusion detection system based on support vector machines and gradually feature removal method," *Expert Systems with Applications*, vol. 39, no. 1, 424–430, 2012, doi:10.1016/j.eswa.2011.07.032.

[54] W. Meng, W. Li, L. Kwok, "Design of intelligent KNN-based

alarm filter using knowledge-based alert verification in intrusion detection," *Security and Communication Networks*, vol. 8, no. 18, 3883–3895, 2015, doi:10.1002/sec.1307.

[55] A. Mahindru, A.L. Sangal, "MLDroid—framework for Android malware detection using machine learning techniques," *Neural Computing and Applications*, vol. 33, 5183–5240, 2020, doi:10.1007/s00521-020-05309-4.

[56] H. Zuhair, A. Selamat, "RANDS: A Machine Learning-Based Anti-Ransomware Tool for Windows Platforms," in *Advancing Technology Industrialization Through Intelligent Software Methodologies, Tools and Techniques*, 573–587, 2019, doi:10.3233/FAIA190081.

[57] U. Adamu, I. Awan, "Ransomware Prediction Using Supervised Learning Algorithms," in *Proceedings of International Conference on Future Internet of Things and Cloud*, Istanbul, Turkey: 1–6, 2019, doi:10.1109/FiCloud.2019.00016.

[58] S. Puthran, K. Shah, "Intrusion Detection Using Improved Decision Tree Algorithm with Binary and Quad Split," in *Proceedings of International Symposium on Security in Computing and Communication*, 427–438, 2016, doi:10.1007/978-981-10-2738-3_37.

[59] J. Zhang, M. Zulkernine, A. Haque, "Random-Forests-Based Network Intrusion Detection Systems," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 38, no. 5, 649–659, 2008, doi:10.1109/TSMCC.2008.923876.

[60] F. Musumeci, A.C. Fidanci, F. Paolucci, F. Cugini, M. Tornatore, "Machine-Learning-Enabled DDoS Attacks Detection in P4 Programmable Networks," *Journal of Network and Systems Management*, vol. 30, no. 21, 2021, doi:10.1007/s10922-021-09633-5.

[61] A.M. Chandrasekhar, K. Raghuveer, "Confederation of FCM clustering, ANN and SVM techniques to implement hybrid NIDS using corrected KDD cup 99 dataset," in *Proceedings of International Conference on Communication and Signal Processing*, Melmaruvathur, India: 1–6, 2014, doi:10.1109/ICCSP.2014.6949927.

[62] S. Ahmed, Z.A. Abbood, H.M. Farhan, B.T. Yasen, M.R. Ahmed, A.D. Duru, "Speaker Identification Model Based on Deep Neural Networks," *Iraqi Journal For Computer Science and Mathematics*, vol. 3, no. 1, 108–114, 2022, doi:10.52866/ijcsm.2022.01.01.012.

[63] A.K. Faieq, M.M. Mijwil, "Prediction of Heart Diseases Utilising Support Vector Machine and Artificial Neural Network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 1, 374–380, 2022, doi:10.11591/ijeecs.v26.i1.pp374-380.

[64] M.M. Mijwil, R.A. Abttan, A. Alkhazraji, "Artificial intelligence for COVID-19: A Short Article," *Asian Journal of Pharmacy, Nursing and Medical Sciences*, vol. 10, no. 1, 1–6, 2022, doi:10.24203/ajpnms.v10i1.6961.

[65] K. Shaukat, S. Luo, V. Varadharajan, I.A. Hameed, S. Chen, et al., "Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity," *Energies*, vol. 13, no. 10, 1–27, 2020, doi:10.3390/en13102509.

[66] D. Chen, P. Wawrzynski, Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustainable Cities and Society*, vol. 66, 102655, 2021, doi:10.1016/j.scs.2020.102655.

[67] P. Suresh, K. Logeswaran, R.M. Devi, K. Sentamilselvan, G.K. Kamalam, H. Muthukrishnan, Contemporary survey on effectiveness of machine and deep learning techniques for cyber security, 177–200, 2022, doi:10.1016/B978-0-323-85209-8.00007-9.

[68] M. Taseer, H. Ghafory, "SQL Injection Attack Detection Using Machine Learning Algorithm," *Mesopotamian Journal of CyberSecurity*, 5–17, 2022, doi:10.58496/MJCS/2022/002.

[69] I.E. Salem, M. Mijwil, A.W. Abdulqader, M.M. Ismaeel, A. Alkhazraji, A.M.Z. Alaabdin, "Introduction to The Data Mining Techniques in Cybersecurity," *Mesopotamian Journal of CyberSecurity*, 28–37, 2022, doi:10.58496/MJCS/2022/004.

[70] R.T. Rasheed, Y. Niu, S.N. Abd, "Harmony Search for Security Enhancement," *Mesopotamian Journal of CyberSecurity*, 5–8, 2021, doi:10.58496/MJCS/2021/002.

[71] T.H.H. Aldhyani, H. Alkahtani, "Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity," *Sensors*, vol. 22, no. 1, 1–20, 2022, doi:10.3390/s22010360.

[72] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, et al., "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," *IEEE Access*, vol. 6, 3491–3508, 2017, doi:10.1109/ACCESS.2017.2782159.

[73] J. Yin, M. Tang, J. Cao, H. Wang, "Apply transfer learning to cybersecurity: Predicting exploitability of vulnerabilities by description," *Knowledge-Based Systems*, vol. 210, 106529, 2020, doi:10.1016/j.knosys.2020.106529.

[74] Z. Tian, C. Luo, J. Qiu, X. Du, M. Guizani, "A Distributed Deep Learning System for Web Attack Detection on Edge Devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, 1963–1971, 2020, doi:10.1109/TII.2019.2938778.

[75] A. Thirumalairaj, M. Jeyakarthic, "Perimeter Intrusion Detection with Multi Layer Perception using Quantum Classifier," in *Proceedings of International Conference on Inventive Systems and Control*, Coimbatore, India: 1–6, 2020, doi:10.1109/ICISC47916.2020.9171159.

[76] K. Atefi, H. Hashim, M. Kassim, "Anomaly Analysis for the Classification Purpose of Intrusion Detection System with K-Nearest Neighbors and Deep Neural Network," in *Proceedings of Conference on Systems, Process and Control*, Melaka, Malaysia: 1–6, 2019, doi:10.1109/ICSPC47137.2019.9068081.

[77] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, 102031, 2020, doi:10.1016/j.simpat.2019.102031.

[78] K. Alrawashdeh, C. Purdy, "Toward an Online Anomaly Intrusion Detection System Based on Deep Learning," in *Proceedings of International Conference on Machine Learning and Applications*, Anaheim, CA, USA: 1–6, 2016, doi:10.1109/ICMLA.2016.0040.

[79] L. Gupta, T. Salman, A. Ghubaish, D. Unal, A.K. Al-Ali, R. Jain, "Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach," *Applied Soft Computing*, vol. 118, 108439, 2022, doi:10.1016/j.asoc.2022.108439.

[80] W. Wang, M. Zhu, X. Zeng, X. Ye, Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in *Proceedings of International Conference on Information Networking*, Da Nang, Vietnam: 1–6, 2017, doi:10.1109/ICOIN.2017.7899588.

Engr. Ramsha Khalid has done her bachelor's degree from Lahore College for Women University, Lahore in 2018. She has done her master's degree from University of Lahore, Lahore in 2022. She is working as Lecturer at University of Sialkot since 2019. Her area of interest includes Computer & Communication Networks, Machine Learning, Artificial Intelligence,

Cyber Security, Control Systems and Renewable Energy Systems. Recently she has published a conference paper in IEEE INMIC'23 held in University of Central Punjab, Lahore as a first author.

Engr. M. Naqi Raza has done his bachelor's degree from University of Gujrat, Gujrat in 2018. He has done his master's degree from University of Sialkot, Sialkot in 2024.

He is working as Junior Lecturer at University of Sialkot since 2019. His area of interest includes Power Generation (Conventional and Renewable), Wind Power Generation and Utilization, Optimization of Wind Energy, Solar Energy, Solar Power Applications, Electric Vehicles (PHEVs).