IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

The Role of Machine Learning in Modern Cybersecurity: An Analysis of Emerging Threats And Defenses

Kundan Kumar Mishra[1] and Dr. Amaravatid Pentaganti[2]
Research Scholar, Department of Computer Science and Engineering[1]
Supervisor, Department of Computer Science and Engineering[2]
NIILM University, Kaithal, Haryana, India

Abstract: *Cybersecurity challenges get increasingly difficult as the world becomes digital. Cyber threats are growing increasingly complex, thus advanced, flexible security techniques are needed. Machine Learning can analyse enormous volumes of data, find trends, and improve threat detection and defence tactics. This research emphasises threat identification and countermeasure execution using machine learning in cybersecurity. Machine learning algorithms in cybersecurity frameworks may expedite decision-making and enable quick responses to dynamic threats. Section 1 discusses cyber threats and the necessity for proactive and effective prevention. Signature-based traditional methods often fail to guard against modern shape-shifting threats. However, machine learning algorithms are better at spotting tiny patterns and abnormalities in vast datasets, making them better at identifying potential threats. Machine learning methods presented in the second part include deep learning, reinforcement learning, and supervised and unsupervised learning. The merits and drawbacks of each threat detection approach are assessed. Data pretreatment and feature engineering improve cybersecurity machine learning models. Machine learning algorithms can adapt to new threats, making them useful cyberwarfare weapons. Successful usage cases from various sectors and cybersecurity applications of machine learning are shown in the last section. ML algorithms identify anomalies and analyse behaviour to reduce false positives and improve security. The paper continues by examining how ML in cybersecurity raises moral issues. Adversarial assaults, skewed datasets, and machine learning model interpretability highlight the need for a holistic strategy that integrates ethics and technology. A more secure and resilient digital future is possible when human expertise and machine intelligence work together to defend against shifting cyberthreats.*

Keywords: Cybersecurity; Machine learning; Threat detection; Defense mechanisms; Anomaly detection

I. INTRODUCTION

Cyberspace's pervasiveness has enabled unprecedented connectedness and efficiency in the digital age, when technology permeates almost every aspect of life [1]. However, the author, Temitayo Oluwaseun, Cyberattacks, from simple viruses to complex, targeted attacks, have increased because to Abraham's interconnection. Strong cybersecurity is crucial as organisations digitise and people grow more reliant on online platforms [1–3].

Traditional cybersecurity, focused on rule-based systems and static signatures, cannot keep up with cyber attackers' advanced techniques [4]. Polymorphic attacks, zero-day exploits, and social engineering make traditional defences ineffective. In this context, Machine Learning (ML) offers optimism and a paradigm change in cybersecurity [5,6].

A subclass of artificial intelligence, machine learning lets computers learn from data and make smart judgements without programming [7–10]. ML's capacity to find patterns, anomalies, and trends in big datasets makes it a powerful cyberdefense tool. Unlike older approaches that use predetermined rules [11], ML algorithms may adapt and change, making them good at discovering new attack routes [12,13].

This study examines the symbiotic link between machine learning and cybersecurity, focusing on threat identification and defence. Understanding the limits of traditional methodologies helps us grasp machine learning's transformational

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

potential [4,14]. The next parts will cover ML methods, their cybersecurity applications, and their ethical implications [15–18].

At the convergence of human brilliance and machine intelligence, ML in cybersecurity promises to strengthen our defences against current attacks and predict and react to upcoming dangers [4]. In this dynamic context, human experience and machine learning's flexibility will reinvent cybersecurity, ushering in an age of resilience, agility, and unmatched protection against ever-changing cyber threats [19,20].

Context of Cybersecurity Challenges

The changing digital environment shapes cybersecurity problems [21]. Cyberattacks get more sophisticated as technology progresses. Digital transformation, adaptive cloud services, IoT devices, and networked systems add to cybersecurity issues. Increasing attack surface susceptibility requires strong security measures to protect digital assets and sensitive data [22,23].

Cybersecurity problems are digital security threats and dangers. Individuals, organisations, and governments confront several cybersecurity issues as technology and networked devices grow. These issues stem from hostile actors, human mistake, technology flaws, and developing cyber threats [24–27].

Cybercrime has increased worldwide [28]. Cybercriminals exploit computer system and network weaknesses using phishing, ransomware, data breaches, identity theft, and financial fraud. Cybercrime has a huge financial effect and evolves as thieves use technology [29–31].

Governments and agencies are common cyber-targets [32]. Nation-states use cyber espionage, IP theft, and sabotage to obtain strategic advantages, destroy infrastructure, or jeopardise sensitive data. These assaults are typically sophisticated and threaten national security. IoT gadgets including smart household appliances, wearables, and industrial control systems pose new security risks. Many IoT devices are vulnerable, which may undermine privacy, secure access, and interrupt vital services [33,34]. The cloud has changed how companies store, analyse, and retrieve data. However, it has raised security worries. Cloud breaches may compromise sensitive data, interrupt services, and violate compliance. To secure cloud infrastructure and data, organisations must take precautions [35,36].

Insiders represent security hazards to an organisation. Disgruntled personnel, negligence, or external threats might cause these dangers. Insiders may compromise systems, disclose critical data, or commit fraud [37]. Social engineering is persuading others to reveal secret information or take security risks [38]. Phishing, pretexting, baiting, and tailgating are used to trick unsuspecting users into giving hackers access to networks or sensitive data [39].

Organisations must follow data protection and privacy laws like the GDPR and CCPA [40]. Multinational organisations have a problem in complying with these requirements and ensuring security. Cybersecurity has potential and difficulties as AI, ML, and blockchain are rapidly used. Threat actors may abuse these technologies, which improve security. These developing technologies need good security [25,39,41].

Strong security policies, user education and awareness, public-private partnership, and continual research and development to keep ahead of new threats are needed to address these cybersecurity issues.

Evolution of Threats in Cyberspace

Cyberattacks aim to compromise computer systems, networks, and data. As cyber threats grow, organisations and people use numerous defences to protect their digital assets. Cyberthreats are always evolving. As technology evolves and we use digital systems more, new hazards arise. Malware, phishing, social engineering, advance persistent threats, supply chain attacks, DoS and DDoS, MitM, SQL injection, XSS, zero-day exploits, and insider threats are common cyber-attacks (Figure 1) and related defence mechanisms [42,43].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

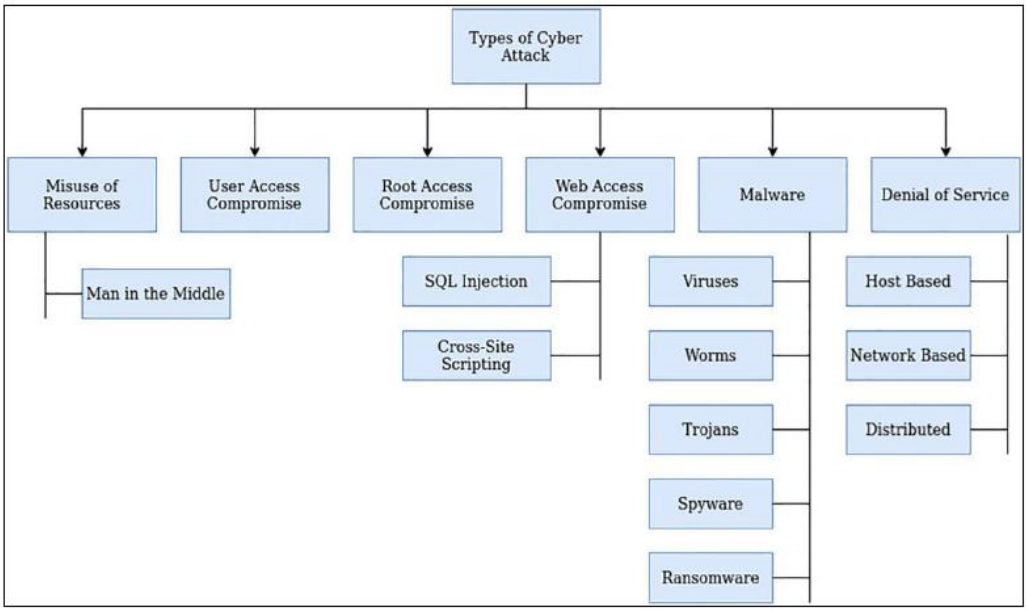

Figure 1 Classifications of cyber-attacks [44]

Since the dawn of computers, viruses, worms, and Trojan horses have been a concern. Malware may steal data, infect systems, and disrupt operations. Phishing attacks impersonate trusted businesses to steal passwords and credit card information. Social engineering uses psychology to trick people into disclosing personal information or doing specified activities [38].

APTs are sophisticated, covert assaults by well-funded, competent cyber adversaries like nation-states. APTs seek long-term access to targeted systems for espionage, data theft, and disruption. Ransomware encrypts data and demands a payment to unlock it. IT assaults on people, corporations, and vital infrastructure are becoming more frequent and destructive [45,46].

With IoT devices' growth, security concerns have surfaced. Insecurely designed or inadequately secured IoT devices may be exploited to get into networks or launch attacks. Supply chain attacks get into trusted software or hardware providers' systems to access their customers' systems. Wide-ranging effects may result from this method [47].

Zero-day exploits attack unpatched software vulnerabilities unknown to the vendor. Cybercriminals or state-sponsored actors use these vulnerabilities to obtain access or spread malware. Internal threats include legitimate users of an organization's systems or data acting maliciously or negligently. These people may leak important information, sabotage systems, or carelessly breach security [37,48].

Security concerns from data breaches, misconfigurations, and unauthorised access to cloud systems have increased as organisations use more cloud services. Both security experts and criminals use AI and ML. Attacks that alter AI models, automated spear-phishing campaigns, and AI-based reconnaissance and attack automation are threats [13,49,50].

Cybersecurity experts, organisations, and governments must modify their defences, use strong security practices, and remain abreast of new attack methods and trends to tackle these growing threats.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

Related Cyber Defense Mechanisms

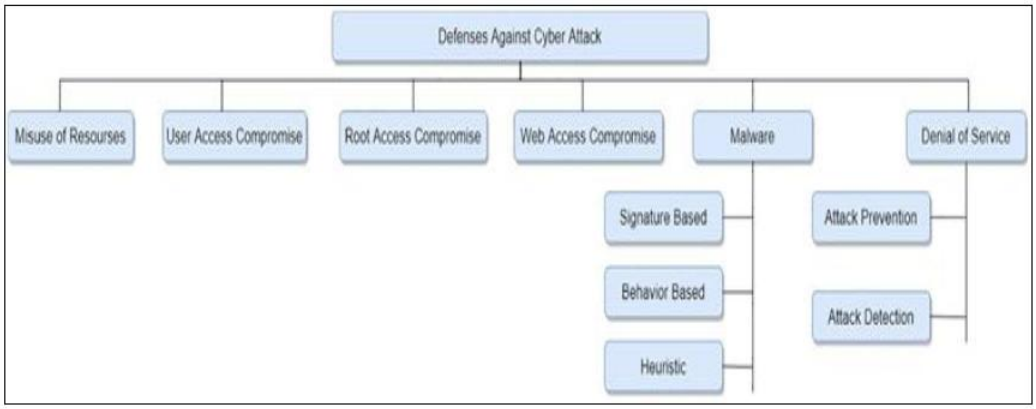

Figure 2 Potential defenses against cyber-attacks [44]

Cyber defence mechanisms safeguard systems, networks, and data against cyberattacks using various methods, technologies, and practices. Firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus and anti-malware software, encryption, multi-factor authentication (mfa), security awareness training, patch management, network segmentation, incident response and cybersecurity policies, and endpoint security are cyber defence mechanisms (Figure 2) [51,52].

Need for Advanced Threat Detection and Defense in Cyberspace

In today's linked world, cyberspace threat detection and defence are more important than ever. Cyber dangers have a large terrain to exploit due to fast technological improvement and digital system dependence. These developing dangers need advanced threat detection and defence methods to identify, reduce, and react.

Cyber attackers use increasingly sophisticated methods and tools to breach systems. Advanced threat detection technologies are needed to identify and protect against these attacks since traditional security measures typically fail. Cyberattacks nowadays use stealth strategies to circumvent detection by standard security measures. Advanced attackers may overcome protection via polymorphic malware, zero-day vulnerabilities, and APTs. These sophisticated and evasive methods are detected by advanced threat detection and defence technologies [45,48].

Cyberattacks often target particular organisations or people. Advanced threat actors may survey and develop targeted attacks, making it difficult for traditional security to detect and stop them. The cyber threat environment changes frequently. New vulnerabilities and attack tactics appear often. Advanced threat detection and defence mechanisms that can adapt to the threat environment, giving a stronger defence against the newest cyber attacks. Internal cyber attacks, whether deliberate or not, pose major hazards to organisations. Advanced threat detection techniques may uncover insider threats and irregularities in user behaviour [53].

With more sensitive data kept online, data and privacy protection are crucial. Organisations can prevent data breaches with advanced threat detection. Many industries must comply with data protection and cybersecurity laws. Advanced threat identification and defence helps organisations follow regulations and avoid legal and financial penalties [54].

Organisations may take a proactive cybersecurity strategy with advanced threat detection and defence technologies. Organisations may minimise cyber-attack damage by recognising and addressing risks early on. Advanced threat detection protects networks and endpoints. A comprehensive strategy that encompasses the network and individual devices is needed to defend against cyber attacks targeting multiple access points [45,55].

Advanced Threat Detection and Defence in cyberspace is needed because cyber threats are evolving, attackers are becoming more sophisticated, and organisations must protect sensitive data, ensure regulatory compliance, and maintain a resilient cybersecurity posture in a dynamic threat landscape.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

Traditional Threat Detection and Defense Mechanism and Associated Drawbacks

Security risks in diverse areas are identified and mitigated using traditional threat detection and defence procedures. These approaches are successful but have downsides [55,56]. Signature-based detection identifies threats using known harmful activity patterns. Antivirus software detects malware using signature databases. Only known threats may be detected using this method. It has trouble handling new or developing threats without signatures. Polymorphic malware and zero-day vulnerabilities may readily escape signature-based detection. Rules or patterns that indicate malicious behaviour are used in rule-based detection. Rule-based IDS detection is common. This method needs manual rule construction and maintenance, which is time-consuming and error-prone. Rule-based systems may also produce false positives or negatives, wasting resources or missing detections.

Network traffic is monitored for suspicious activity or abnormalities. It may struggle with encrypted traffic or application-layer assaults, although it can identify network-based attacks. The amount of notifications from network-based detection may overload security professionals and make it hard to concentrate on serious risks. Host-based detection monitors system or host actions and events. It may reveal system-level breaches and malicious activity. However, host-based detection is restricted to host visibility. Multiple-system assaults or network lateral movement may go unnoticed. Many classic threat detection techniques use human analysts to analyse warnings, investigate occurrences, and make conclusions. Manual processing takes time and might be error-prone. Analysts may overlook tiny signs of an assault or struggle to keep up with automatic detection systems' notifications.

Traditional techniques sometimes lack context and behaviour analysis. They may ignore the context of an assault or advanced threat behaviour patterns in favour of static signs. This may cause missed detections or failure to identify complex low-and-slow or multi-stage assaults. Traditional systems may struggle with scalability and performance. As data volume and threat complexity rise, these processes may struggle to process, delaying detection and action.

Organisations are using machine learning-based anomaly detection, behaviour analytics, threat intelligence sharing, and security automation and orchestration to overcome these restrictions. These methods use AI and automation to increase detection accuracy, decrease false positives, and speed up threat response.

Machine Learning for Threat Detection in Cybersecurity

Machine Learning (ML) uses a variety of methods and algorithms to help computers understand patterns, forecast, and improve performance without being programmed. Supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning, deep learning, neural networks, decision trees, random forests, support vector machines (SVM), and K-Nearest neighbours (KNN) can be used for classification, clustering, regression, or other purposes [57].

Machine learning (ML) is a potent cybersecurity threat detection technology. It lets you build strong and adaptable systems that can analyse massive volumes of data, find trends, and spot security concerns. Cybersecurity threat detection often uses ML. Machine learning algorithms can find patterns and attributes in malware samples. This information may be utilised to create models that identify new malware strains by matching patterns.

ML may develop models that learn "normal" system or network behaviour. These algorithms can then detect abnormal behaviour that may signal a cyberattack. ML may detect unusual network traffic irregularities that may signal an intrusion attempt. These algorithms identify new attack patterns by learning from past data.

ML may detect irregularities in login timings, access patterns, and resource consumption that may suggest compromised accounts or insider threats. Phishing and spam email patterns may be learned by ML systems. These models can detect and filter harmful information. ML can detect DDoS and botnet trends in network traffic.

ML may rank vulnerabilities by severity and effect. Machine learning models may assist security teams prioritise key vulnerabilities by analysing historical data and vulnerability scan findings.

Machine learning may help identify threats, but it is not a single solution. It should be utilised alongside frequent patching, secure setups, and user training to form a strong cybersecurity approach. Machine learning models must be monitored and updated to react to changing threats and minimise false positives and negatives.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

Recommendation

Continuous research is needed to improve machine learning's cyber threat detection accuracy. Threat detection, categorisation, and response may be automated using machine learning to improve cybersecurity. Machine learning models understand patterns and generate accurate predictions using well-labeled and varied training data. A complete and up-to-date inventory on cyber dangers, both known and emergent, is essential. Cyber dangers must be represented by appropriate qualities or attributes. Cybersecurity domain knowledge and experience may assist choose and develop significant features that capture threat kinds. Ensemble learning predicts using many machine learning models. Ensemble approaches increase accuracy and generalisation by pooling model outputs. Using bagging, boosting, and stacking may generate varied and strong ensembles.

New risks may be found via anomaly detection. Machine learning models may identify risks by learning regular behaviour patterns. Anomaly detection often uses clustering, autoencoders, and one-class SVMs. Deep learning models like CNNs and RNNs have shown success in cybersecurity and other fields. These algorithms understand complicated data patterns and correlations to identify threats accurately. Cyber risks evolve, thus old data models may be obsolete. Continuous learning helps the model to adapt and update its expertise with new threat information in real time, enhancing threat detection accuracy. Threat actors use adversarial assaults to avoid machine learning analyses. Adversarial machine learning creates models that can survive assaults. Adversarial training, defensive distillation, and input sanitization improve model robustness. Machine learning algorithms can automate and improve threat detection, but humans are still needed. Human and domain expertise may check and understand model predictions, enhancing accuracy and lowering false positives/negatives. Machine learning models must be regularly assessed to find areas for development. Analysts and cybersecurity specialists may help improve model accuracy over time.

Machine learning can improve cyber threat identification, but it should be part of a comprehensive cybersecurity framework that includes network monitoring, intrusion detection systems, secure coding, and user awareness training.

II. CONCLUSION

Cybersecurity paradigm shifts with ML-based proactive defence. ML makes defence more intelligent, adaptable, and efficient by using sophisticated analytics and pattern recognition. ML's capacity to identify small abnormalities, automate actions, and learn from emerging threats makes it essential to current cybersecurity. Analysing massive amounts of data using machine learning and AI algorithms may reveal trends, abnormalities, and new risks. Machine learning models may learn threat patterns from past data and improve over time.

ML integration in proactive defence measures is a strategic requirement for organisations trying to remain ahead of cyber attackers, notwithstanding obstacles. ML's full potential in cybersecurity defences will depend on resolving issues and using its capabilities as the area evolves.

REFERENCES

[1]. M.R. Kearney, Navigating the Eisenhower Interstate System: Paving the way for cyberspace, Explor. Media Ecol. 22 (2023) 33–48.
[2]. Nassar, M. Kamal, Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies, J. Artif. Intell. Mach. Learn. Manag. 5 (2021) 51–63.
[3]. M. Abdel-Rahman, Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world, Eig. Rev. Sci. Technol. 7 (2023) 138–158.
[4]. D.P.F. Möller, Cybersecurity in Digital Transformation, in: Guid. to Cybersecurity Digit. Transform. Trends,Methods, Technol. Appl. Best Pract., Springer, 2023: pp. 1–70.
[5]. K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, T. Tran, Grand challenge: Applying artificial intelligence and machine learning to cybersecurity, Computer (Long. Beach. Calif). 52 (2019) 45–52.
[6]. I.D. Aiyanyo, H. Samuel, H. Lim, A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning, Appl. Sci. 10 (2020). https://doi.org/10.3390/app10175811.
[7]. S. Raschka, J. Patterson, C. Nolet, Machine learning in python: Main developments and technology trends in datascience, machine learning, and artificial intelligence, Information. 11 (2020) 193.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

[8]. F. Chinesta, E. Cueto, Empowering engineering with data, machine learning and artificial intelligence: a short introductive review, Adv. Model. Simul. Eng. Sci. 9 (2022) 21.
[9]. Nassehi, R.Y. Zhong, X. Li, B.I. Epureanu, Review of machine learning technologies and artificial intelligence in modern manufacturing systems, in: Des. Oper. Prod. Networks Mass Pers. Era Cloud Technol., Elsevier, 2022: pp. 317–348.
[10]. O.K. Ukoba, B. Eng, U.S. Anamu, O. Ogundare, M. Eng, M.C. Ibegbulam, O.A. Akintunlaji, A Model to Predict the Inhibitive Property of PKO on Crude Oil Pipeline ., 12 (2011) 39–44.
[11]. U.S. Anamu, O.O. Ayodele, E. Olorundaisi, B.J. Babalola, P.I. Odetola, A. Ogunmefun, K. Ukoba, T.-C. Jen, P.A. Olubambi, Fundamental design strategies for advancing the development of high entropy alloys for thermo- mechanical application: A critical review, J. Mater. Res. Technol. (2023). https://doi.org/https://doi.org/10.1016/j.jmrt.2023.11.008.
[12]. Y. Wang, T. Sun, S. Li, X. Yuan, W. Ni, E. Hossain, H.V. Poor, Adversarial Attacks and Defenses in Machine Learning- Empowered Communication Systems and Networks: A Contemporary Survey, IEEE Commun. Surv. Tutorials. (2023).
[13]. E. Bout, V. Loscri, A. Gallais, How Machine Learning changes the nature of cyberattacks on IoT networks: A survey, IEEE Commun. Surv. Tutorials. 24 (2021) 248–279.
[14]. N.D. Trung, D.T.N. Huy, T.-H. Le, IoTs, machine learning (ML), AI and digital transformation affects various industries-principles and cybersecurity risks solutions, Management. 18 (2021).
[15]. S. Al-Mansoori, M. Ben Salem, The role of artificial intelligence and machine learning in shaping the future of cybersecurity: trends, applications, and ethical considerations, Int. J. Soc. Anal. 8 (2023) 1–16.
[16]. R.H. Jhaveri, A. Revathi, K. Ramana, R. Raut, R.K. Dhanaraj, A review on machine learning strategies for real-world engineering applications, Mob. Inf. Syst. 2022 (2022).
[17]. O. Alshaikh, S. Parkinson, S. Khan, Exploring Perceptions of Decision-Makers and Specialists in Defensive Machine Learning Cybersecurity Applications: The Need for a Standardised Approach, Comput. Secur. (2023) 103694.
[18]. V. Velayutham, S. Kumar, A. Kumar, S. Raha, G.C. Saha, Analysis of Deep Learning in Real-World Applications: Challenges and Progress, Tuijin Jishu/Journal Propuls. Technol. 44 (n.d.) 2023.
[19]. J. Bharadiya, Machine Learning in Cybersecurity: Techniques and Challenges, Eur. J. Technol. 7 (2023) 1–14.
[20]. K. Shaukat, S. Luo, V. Varadharajan, I.A. Hameed, S. Chen, D. Liu, J. Li, Performance comparison and current challenges of using machine learning techniques in cybersecurity, Energies. 13 (2020) 2509.
[21]. M.T. Nguyen, M.Q. Tran, Balancing Security and Privacy in the Digital Age: An In-Depth Analysis of Legal and Regulatory Frameworks Impacting Cybersecurity Practices, Int. J. Intell. Autom. Comput. 6 (2023) 1–12.
[22]. Djenna, S. Harous, D.E. Saidouni, Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure, Appl. Sci. 11 (2021) 4580.
[23]. Lakhani, AI Revolutionizing Cyber security unlocking the Future of Digital Protection, (2023).
[24]. T. Krause, R. Ernst, B. Klaer, I. Hacker, M. Henze, Cybersecurity in power grids: Challenges and opportunities, Sensors. 21 (2021) 6225.
[25]. F.R. Bechara, S.B. Schuch, Cybersecurity and global regulatory challenges, J. Financ. Crime. 28 (2021) 359–374.
[26]. F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, M. Michaloliakos, Cybersecurity challenges in the maritime sector, Network. 2 (2022) 123–138.
[27]. S. Tufail, I. Parvez, S. Batool, A. Sarwat, A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid, Energies. 14 (2021) 5894.
[28]. S. Gangwar, V. Narang, A Survey on Emerging Cyber Crimes and Their Impact Worldwide, in: Res. Anthol. Combat. Cyber-Aggression Online Negativity, IGI Global, 2022: pp. 1583–1595.
[29]. G. Sarkar, H. Singh, S. Kumar, S.K. Shukla, Tactics, techniques and procedures of cybercrime: A methodology and tool for cybercrime investigation process, in: Proc. 18th Int. Conf. Availability, Reliab. Secur., 2023: pp. 1–10.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

[30]. M. Bada, J.R.C. Nurse, Profiling the cybercriminal: a systematic review of research, in: 2021 Int. Conf. Cyber Situational Awareness, Data Anal. Assess., IEEE, 2021: pp. 1–8.
[31]. G. Sarkar, S.K. Shukla, Behavioral analysis of cybercrime: Paving the way for effective policing strategies, J. Econ.Criminol. (2023) 100034.
[32]. J. Chigada, R. Madzinga, Cyberattacks and threats during COVID-19: A systematic literature review, South African J. Inf. Manag. 23 (2021) 1–11.
[33]. M. Alsheikh, L. Konieczny, M. Prater, G. Smith, S. Uludag, The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders, IEEE Consum. Electron. Mag. 11 (2021) 59–68.
[34]. G. Fortino, A. Guerrieri, P. Pace, C. Savaglio, G. Spezzano, Iot platforms and security: An analysis of the leading industrial/commercial solutions, Sensors. 22 (2022) 2196.
[35]. R. Frank, G. Schumacher, A. Tamm, The Cloud Transformation, in: Cloud Transform. Public Cloud Is Chang. Businesses, Springer, 2023: pp. 203–245.
[36]. Berisha, E. Mëziu, I. Shabani, Big data analytics in Cloud computing: an overview, J. Cloud Comput. 11 (2022) 24.
[37]. S. Yuan, X. Wu, Deep learning for insider threat detection: Review, challenges and opportunities, Comput. Secur.104 (2021) 102221.
[38]. W. Syafitri, Z. Shukur, U. Asma'Mokhtar, R. Sulaiman, M.A. Ibrahim, Social engineering attacks prevention: A systematic literature review, IEEE Access. 10 (2022) 39325–39343.
[39]. Moallem, Cybersecurity, Privacy, and Trust, Handb. Hum. Factors Ergon. (2021) 1107–1120.
[40]. P. Mulgund, B.P. Mulgund, R. Sharman, R. Singh, The implications of the California Consumer Privacy Act (CCPA)on healthcare organizations: Lessons learned from early compliance experiences, Heal. Policy Technol. 10 (2021) 100543.
[41]. Mishra, Y.I. Alzoubi, A.Q. Gill, M.J. Anwar, Cybersecurity enterprises policies: A comparative study, Sensors. 22 (2022) 538.
[42]. Dobák, Thoughts on the evolution of national security in cyberspace, Secur. Def. Q. 33 (2021) 75–85.
[43]. M. Kopczewski, Z. Ciekanowski, J. Nowicka, K. Bakalarczyk-Burakowska, Security threats in cyberspace, Sci. J. Mil. Univ. L. Forces. 54 (2022).
[44]. K.A. Al-Enezi, I.F. Al-Shaikhli, A.R. Al-Kandari, L.Z. Al-Tayyar, A survey of intrusion detection system using case study Kuwait Governments entities, in: 2014 3rd Int. Conf. Adv. Comput. Sci. Appl. Technol., IEEE, 2014: pp. 37– 43.
[45]. Sharma, B.B. Gupta, A.K. Singh, V.K. Saraswat, Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures, J. Ambient Intell. Humaniz. Comput. (2023) 1–27.
[46]. F. Teichmann, S.R. Boticiu, B.S. Sergi, The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate?, Int. Cybersecurity Law Rev. 4 (2023) 259–280.
[47]. Z. Li, Y. Ge, J. Guo, M. Chen, J. Wang, Security threat model under internet of things using deep learning and edge analysis of cyberspace governance, Int. J. Syst. Assur. Eng. Manag. 13 (2022) 1164–1176.
[48]. О.С. Саприкін, Models and methods for diagnosing Zero-Day threats in cyberspace, Вісник Сучасних Інформаційних Технологій. 4 (2021) 155–167.
[49]. Panem, S.R. Gundu, J. Vijaylaxmi, The Role of Machine Learning and Artificial Intelligence in Detecting the Malicious Use of Cyber Space, Robot. Process Autom. (2023) 19–32.
[50]. Malaviya, Application of machine learning and artificial intelligence for securing cyber space and the role of government organization, Anusandhaan-Vigyaan Shodh Patrika. 10 (2022) 33–37.
[51]. S. Vyas, J. Hannay, A. Bolton, P.P. Burnap, Automated Cyber Defence: A Review, ArXiv Prepr. ArXiv2303.04926. (2023).
[52]. H.T. Reda, A. Anwar, A.N. Mahmood, Z. Tari, A Taxonomy of Cyber Defence Strategies Against False Data Attacks in Smart Grids, ACM Comput. Surv. 55 (2023) 1–37.
[53]. D.C. Le, N. Zincir-Heywood, Exploring anomalous behaviour detection and classification for insider threat identification, Int. J. Netw. Manag. 31 (2021) e2109.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, October 2024

[54]. Y. Mirsky, A. Demontis, J. Kotak, R. Shankar, D. Gelei, L. Yang, X. Zhang, M. Pintor, W. Lee, Y. Elovici, The threat of offensive ai to organizations, Comput. Secur. 124 (2023) 103006.
[55]. M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, N. Ghadimi, A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future, Electr. Power Syst. Res. 215 (2023) 108975.
[56]. W. Ahmad, A. Rasool, A.R. Javed, T. Baker, Z. Jalil, Cyber security in IoT-based cloud computing: A comprehensive survey, Electronics. 11 (2021) 16.
[57]. I.H. Sarker, Machine learning: Algorithms, real-world applications and research directions, SN Comput. Sci. 2 (2021) 160.