e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 12, December 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612055|

A Thorough Evaluation of AI-Driven Detection for Enhancing Cybersecurity

Vikesh Kumar Singh, Dr. Istiyaque Ahmad

Scholar, Department of Computer Science, Sunrise University, Alwar, India

Research Supervisor, Assistant Professor, Department of Computer Science, Sunrise University, Alwar, India

ABSTRACT: Good methods to identify and prevent cyberattacks are more critical than ever before due to the exponential growth in both the frequency and sophistication of such assaults. Because cybercriminals may inflict enormous harm to both people and companies, it is critical that they be identified promptly and correctly. To better identify cyber-attacks, this study examines how artificial intelligence (AI) techniques like deep learning (DL) and machine learning (ML) may be used in conjunction with metaheuristic algorithms. For this purpose, we have reviewed sixty current papers to determine the efficacy of these AI systems in detecting and countering various cyber threats. Using a wide variety of cyberattacks—malware, network intrusions, spam, and more—our study demonstrates that ML/DL methodologies, in conjunction with metaheuristic algorithms, greatly enhance our ability to detect and react to cyber threats. In order to better prepare for new and evolving cyber-attacks, we examine several AI algorithms to identify their strengths and areas for improvement. This study lays forth a simple methodology for evaluating AI techniques for cyber threat identification. It is vital to improve AI approaches and consistently provide effective security due to the growing complexity of cyber threats. We take a look at the metaheuristic algorithms, as well as the present ML and DL models, and assess their strengths and weaknesses. It is critical to acknowledge these limitations in order to direct future improvements. Our focus is on finding innovative and adaptable solutions that can tackle any problem that comes our way. Our study indicates that in order to prevent cyberattacks in the future, it will be necessary to update AI systems often to keep up with hackers' current techniques.

KEYWORDS: Cyber-attacks, Artificial intelligence, Machine learning, Deep learning,Cyber security, Intrusion detection.

I. INTRODUCTION

The internet has grown at an astounding rate despite the emergence of new digital technologies including software-defined networking (SDN), big data, and fog computing. Critical infrastructure is particularly vulnerable to the cybersecurity threats posed by these innovations. The complex nature of modern cyber threats has made it difficult for traditional security solutions, which depend on fixed security controls such as intrusion detection and prevention systems and firewalls, to stay up with the times [1]. The advent of Deep Learning (DL) has been revolutionary, opening up new avenues for data accessibility, improved performance, and potential maximisation.

transformed not only the use of artificial intelligence (AI) in picture, speech, and behavioural analytic applications, but also paved the way for revolutionary developments in robotics, speech recognition, and face recognition, among other fields. Deep learning has developed into an essential tool for cybersecurity professionals, helping to identify breaches and keep an eye out for malware. This is a significant improvement above previous ML applications [2]. The dependence on human feature extraction has become an apparent drawback of ML, especially in the realm of cybersecurity, despite its seeming promise. One example is the time-consuming and error-prone process of manually compiling malware features for ML-based identification. This approach ignores unknown characteristics and limits the effectiveness of threat detection to established features. Consequently, the accuracy of feature extraction and recognition is crucial to ML's performance. Discovering complicated, nonlinear connections within data gives DL a strategic advantage in cyber defence by allowing the discovery of new filetypes and previously undisclosed threats. Most notably, DL has accelerated progress in preventing Advanced Persistent Threat (APT) assaults, which can even identify the most elusive methods' subtle, high-level traits.

Cybersecurity is now at the forefront of modern security discussions due to the proliferation of connected devices, the proliferation of the Internet of Things (IoT), and several related applications. There has never been a more critical time to build strong intrusion detection systems and efficiently identify a range of cyber threats [4]. Many companies are now

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612055|

using cloud computing to outsource their data and computational needs, which has increased the need of having a secure platform, especially for cloud-based systems. With cybersecurity data being so large and diverse, it is crucial to understand virus behaviour in the context of behavioural space in order to improve the efficacy of conventional security measures [5]. To build advanced intrusion detection systems, ML is leading the charge in automating behaviour analysis by extracting useful features from network packets. Giving computers the capacity to learn and adapt independently, without human intervention, is the heart of ML [6]. In today's world, where cybersecurity encompasses many policies, processes, and methods that try to protect the confidentiality and integrity of data, the objective is to lessen the likelihood of attacks and prevent unauthorised access. Systems that can detect major signs of possible breaches are urgently needed due to the increasing frequency and sophistication of assaults.Although DL is complicated, it has the potential to give accurate results when trained correctly, which would be a huge improvement in cybersecurity approaches [6].Examining the use of DL, ML, and Metaheuristics in contemporary cybersecurity practices, this article seeks to assess their efficacy in countering cyber-attack risks and to suggest avenues for further study and use.

II. RESEARCH OBJECTIVES

Due to the frequency and complexity of current cyber attacks, the cybersecurity environment is confronted with new problems in today's fast evolving digital world. The ever-changing and intricate nature of modern threats renders traditional security measures like intrusion detection systems and firewalls useless. These systems depend on static controls and human operations. There is a strong need for human involvement, sluggish reaction times, and a high risk of false positives since these approaches do not identify modern tactics like as malware, phishing, APTs, botnets, and insider threats.This study is driven by the pressing need to fill the void that these conventional approaches have created. In order to handle massive volumes of data in real-time, detect complex patterns, and swiftly react to new dangers, we want to tap into the potential of AI by investigating AI-driven approaches, particularly DL and ML. Artificial intelligence's capacity to learn from data and evolve over time makes it a priceless asset in the fight against cybersecurity threats. These include botnets, which are networks of infiltrated devices controlled by bad actors who can launch coordinated assaults that overwhelm conventional defences, and insider threats, which originate from within the organisation and are thus difficult to detect using conventional methods.The three primary areas of machine learning (ML), deep learning (DL), and metaheuristic technologies (MT) need to be covered extensively in many surveys. Furthermore, they often exclude portions devoted to future work and restrictions or do not cover the whole range of cyber-attacks.Our study, on the other hand, covers all of these bases extensively, down to the sections that address limits and suggestions for further research. In addition, we have included all current datasets with their respective papers to guarantee that our survey is based on the most recent research.

The overarching goal of this study is to prove that AI has the potential to revolutionise cybersecurity by making defences more precise, efficient, and adaptable. Our goal is to develop a more secure digital environment by improving the detection and mitigation of advanced cyberthreats, such as botnets and insider threats, by utilising AI's strengths and overcoming the shortcomings of traditional methods, like static controls and manual feature extraction.

III. METHODOLOGY

Primary result. A comprehensive overview of current research on various cyber-attacks and the technology used to detect them is the main contribution of this study. It gives researchers an overview of the field and lays the groundwork for future studies on the use of AI to identify and lessen cyber dangers by outlining existing difficulties and knowledge gaps in the field. The research's contributions are categorised as follows:

• An examination of anomaly detection, classification, and analysis methodologies as well as ML, DL, and metaheuristic approaches to cyber-attack detection. Cybersecurity and the use of basic AI techniques were the topics of sixty academic publications reviewed and critically examined throughout the last four years. Evaluation of open-access cyber-security datasets and primary classification of cyber-attack types found within these datasets. Data sets. Methods for reducing data complexity. Ways of sorting data. Methods for comparison. Performance measurement. You may easily comprehend the different methodologies and results by referring to the comparison tables that organise the research' essential aspects.

A conclusion that addresses the challenges encountered with these AI methods in cybersecurity and proposes future solutions.

Framework for papers is to provide a systematic exploration of AI approaches in cyber-attack detection, the study is organised into six parts with distinct headings. We provide the research's contributions and reasons for doing the study

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612055|

in the "Introduction" section. We explain the research's context and outline its primary themes in the "Background" section. We evaluate relevant literature in the 'LiteratureReview' section.

IV. BACKGROUND

The expansion of computer networks has changed the way societies operate, resulting in a rise in the number and sophistication of cyberattacks. Cyberattacks are operations that harm computer systems, networks, or data by targeting them. They are often well-organised and well-planned, and they need a series of coordinated procedures to reach their objectives [3]. These insider threats are a significant and growing part of these attacks. They are usually carried out by disgruntled or rogue employees who exploit their authorised access to steal data or cause harm. They do this with the intention of causing damage, unauthorised access, or service interruptions that result in severe data loss or financial damage, which often leads to long-lasting consequences [7]. These dangers might also come from unwanted programs that people unintentionally install on their devices. These apps can access and abuse critical information. To counteract these attacks, advanced behavioural anomaly detection and auto-resiliency methods are being developed to proactively identify and mitigate harmful activities at both the personnel and application levels [8].

There are many different types of cyberattacks that pose a wide range of dangers in the digital world. Table 1 summarises the information that is highlighted in the literature, which provides insights into numerous essential forms of these assaults. This material highlights the complexity and variety of cyber dangers, demonstrating the many assaults that organisations and people may face in today's networked world [3]. Botnets are another serious cyber hazard. They are networks of compromised computers that are controlled by an attacker to carry out coordinated malicious operations, such as DDoS assaults, data theft, and spamming. These networks may be quite large, consisting of hundreds or even millions of hacked devices, which makes it extremely difficult to break them apart. Botnet operators utilise advanced strategies to infect devices and keep control over them, constantly changing their tactics in order to avoid being detected [9].The variety of cyber-attack kinds demonstrates the critical need of having good cybersecurity procedures. It is essential to protect sensitive information and ensure that digital services are functioning properly. These forms of cyberattacks are classified in Figure 1. It is important to be vigilant and keep investing in modern security solutions since cyber threats are always evolving. In order to stay ahead of cyber threats, it is necessary to actively adjust to emerging risks, utilise best practices, and take use of technology to protect against the various strategies employed by attackers [11].The cybersecurity community has actively concentrated on attack detection as a cor-nerstone technique in response to these expanding threats. This method keeps a close watch on network activity, system state, and use patterns in order to proactively detect and eliminate unauthorised access or assaults. In this context, artificial intelligence (AI) and its subsets, such as machine learning (ML) and deep learning (DL), provide potential options to assist with cybersecurity. Because of its ability to quickly develop and manage vast amounts of data, AI is a good choice for detecting and reacting to complex cyber threats. Artificial intelligence systems may identify malware, insider threats, botnets, network intrusions, phishing attempts, and other harmful behaviours by analysing patterns and learning from experience [12].

Artificial intelligence (AI) is the science and engineering of creating intelligent robots. The term was first defined by pioneers like John McCarthy in 1956 [13]. Artificial intelligence has developed into a fundamental aspect of computer science over the years. It focusses on imitating the way humans think by utilising complicated mathematical algorithms. This branch of study integrates elements from several disciplines in order to create computers that are capable of learning, reasoning, and making decisions depending on the data they process. Additionally, it includes the reproduction of human cognition and behaviour in computers, which are categorised as thinking and responding both humanly and logically [14]. AI applications span from basic jobs tocomplex problem-solving sectors such as cybersecurity, where it confronts sophisti-cated cyber threats. This revolutionary technology is constantly expanding the limits of what robots can do, with the goal of improving human skills and automating activities using aided, augmented, and autonomous intelligence [15].

V. LITERATURE REVIEW

Recent developments in computer technology, especially artificial intelligence, have had a major effect on daily life and work by creating systems that can do jobs that used to need human intellect. AI systems are very good at analysing data and making decisions in real time. They use large amounts of data to tackle complicated issues in many different scientific and technical fields. This skill is becoming more and more important in cybersecurity, where the large amount of data makes it impossible to analyse it manually, and the complexity of threats, particularly those based on artificial intelligence, is constantly changing. Using artificial intelligence may significantly lower the costs and time required to construct threat identification algorithms, even though hiring specialists can be expensive [15]. Artificial intelligence has many different roles in cybersecurity. It comprises the effective and precise analysis of enormous data sets, using previous

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612055|

threat data to predict and reduce the impact of future attacks, even when the methods used to carry out assaults change. Because of its capacity to adapt, AI is a very useful tool for cyber defence. It has the ability to recognise important changes in attack patterns, handle enormous amounts of data, and increase ongoing learning in AI security systems in order to enhance threat response [34]. On the other hand, it is difficult to use artificial intelligence in cybersecurity. In order to work properly, AI systems need a lot of data, and processing so much data might take a lot of resources. In addition, the possibility of false alerts may reduce user confidence in AI systems, and delayed reactions to threats might affect the efficacy of the system [34]. In addition, cyber-attacks pose a serious threat to security systems that are based on artificial intelligence. Ongoing research is improving the ability of AI to withstand cyberattacks, even with these challenges. Our survey covers a wide range of artificial intelligence techniques, including machine learning, deep learning, and metaheuristic algorithms, in order to address a variety of cyber threats, such as malware, network intrusions, insider threats, botnets, and spam. It also includes over sixty recent studies and a comparison of multiple AI methodologies. We make sure that our poll covers the three primary aspects of machine learning, deep learning, and metaheuristic technologies in detail, which is not the case for many other surveys. In addition, we cover a broad range of cyber-attacks and provide specific areas for future studies and limitations, which is something that many surveys do not include. Additionally, it has a comprehensive list of current datasets and the papers that correlate to them, which guarantees that our conclusions are based on the most up-to-date research. Using a variety of benchmark datasets guarantees thorough validation. The article emphasises the practical integration of artificial intelligence (AI) and machine learning (ML) models in a variety of contexts, including the Internet of Things (IoT), cloud computing, and conventional networks. As a result, its conclusions are extremely applicable. It also emphasises practical benefits such as automation and real-time attack response, demonstrating how artificial intelligence may be useful in cybersecurity. The future recommendations are thorough and practical, concentrating on ongoing improvement, the creation of new datasets, openness, explainability, and the early incorporation of artificial intelligence into the cybersecurity lifecycle in order to take preventative steps. In [35], applications of artificial intelligence (AI), machine learning (ML), deep learning (DL), and reinforcement learning (RL) in cybersecurity are discussed. These applications include malware detection, intrusion detection, and vulnerability assessment. However, it might benefit from looking at how AI and blockchain can be used to improve data integrity, as well as real-world case studies for practical insights. It is necessary to do a thorough comparison with conventional procedures and to have conversations about legal and ethical factors as well as privacy concerns. Focussing on human-AI collaboration, resilience against adversarial assaults, and cross-disciplinary techniques would provide a more comprehensive view. It is also important to consider the future development of artificial intelligence in order to deal with new threats, scalability, deployment issues, and organisational preparedness, which includes the training that cybersecurity specialists need. These enhancements would make the research more thorough and realistic for the use of artificial intelligence and machine learning in cybersecurity. A thorough analysis of AI system vulnerabilities to cyberattacks is presented in [36]. The report classifies these threats into two categories: manipulation attacks and extraction assaults. The technol ogies presented include ML, DL, and different defence mechanisms such as adversarial training, feature squeezing, and robust aggregation approaches. The study describes many sorts of assaults, including adversarial attacks, poisoning attacks, model inversion, and extraction attacks. A variety of benchmark datasets are used for comprehensive validation, however just one particular area has been presented. A thorough grasp of the present state of research in artificial intelligence and cybersecurity has been achieved via a comparative examination of various major studies. The comparison includes a variety of factors, such as the purpose and scope, methodology, data sources, and situations in which the data was utilised. This analysis emphasises the unique methods and results of each study, which helps to place the current research within the larger framework of the existing body of literature. In [37], there is a thorough examination of the ways in which artificial intelligence and machine learning are used in cybersecurity. Supervised learning for intrusion detection, malware detection, and network security are some of the most important technologies. Methods of unsupervised learning that are used to detect new dangers. The article discusses applications such as security automation, threat intelligence, vulnerability management, and security education, which include malware, intrusion attempts, ransomware, crypto-jacking, and IoT assaults. However, it is still necessary to include a range of approaches for detecting cyberattacks. A comprehensive review of AI applications in cybersecurity is presented in [38], which organises 236 papers according to the NIST framework. It demonstrates AI's importance in automating processes, strengthening threat detection, and improving response accuracy utilising ML, DL, natural language, and RL technologies. The most important categories are asset management, threat hunting, vulnerability assessment, incident response, and dealing with malware, phishing, advanced persistent threats, and insider threats. The research covers a lot of ground, but it still requires more consideration of practical deployment issues, ethical consequences, and possible biases in AI models. It should also involve conversations on standardised benchmarks and assessment measures for determining how successful AI is. Future research should concentrate on these elements in order to guarantee that artificial intelligence applications in cybersecurity are both effective and ethical.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612055|

Some research has focused on discovering software vulnerabilities and malware, which are two areas where AI may have a large influence. In order to enhance malware detection and software security, a variety of techniques have been widely used, including data mining, machine learning classifiers such as K-nearest neighbours (KNNs) and support vector machines (SVMs), deep learning architectures, and metaheuristic algorithms [39]. To address cybersecurity in the Internet of Things (IoT) environment, Asiri et al. presented the Hybrid Metaheuristics Feature Selection with Stacked DL Enabled Cyber-Attack Detection (HMFS-SDLCAD) model. They use a new method that combines Salp Swarm Optimisation based on PSO (SSOPSO) for feature selection and a Stacked Bidirectional Gated Recurrent Unit (SBiGRU) for identifying and categorising cyber-attacks. The Whale Optimisation Algorithm (WOA) is also used by the model to optimise the hyperparameters. This whole system, which has been verified against benchmark datasets, has shown significant improvements over current models, proving that it is effective in detecting cyber-attacks in real time [40]. Caviglione et al. provide a comprehensive examination of the current malware threats, demonstrating that assaults are becoming more complex as a result of technology improvements and new techniques of exploitation. The article emphasises the increasing number of malware assaults that are being carried out by cybercriminals who are looking to make money with a lower risk than conventional crimes. The paper also examines the difficulties of detecting current malware because of the variety and complexity of assaults, emphasising the necessity for detection systems to constantly evolve. The authors examine the current situation regarding malware and its detection, with an emphasis on machine learning methods, which are becoming more popular as a way to fight against the fast development of malware. Their study highlights the need to keep ahead in the continuous arms race between attackers and defenders in the realm of cybersecurity [41]. An et al. revolutionised the area of cyber security by inventing a CNN-based model (V-CNN) for the automated discovery of vulnerabilities, using DL to surpass conventional static analysis. They used a whole dataset from MITRE's CVE/CWE and redefined vulnerabilities in order to improve detection in their technique.

VI. DISCUSSION

AI and Cybersecurity: A Comprehensive Overview

- AI systems are adept at real-time data analysis and decision-making, making them crucial in cybersecurity.
- AI's ability to adapt and handle large data sets makes it a valuable tool for cyber defense.
- AI can recognize changes in attack patterns, handle large data sets, and enhance threat response.
- Challenges include the need for large amounts of data, potential false alerts, and delayed responses to threats.
- Ongoing research is aimed at improving AI's ability to withstand cyberattacks.
- The survey covers various AI techniques, including machine learning, deep learning, and metaheuristic algorithms, to address various cyber threats.
- The survey includes over sixty recent studies and a comparison of multiple AI methodologies.
- The article emphasizes the practical integration of AI and machine learning models in various contexts, including IoT, cloud computing, and traditional networks.
- Future recommendations focus on ongoing improvement, creation of new datasets, openness, explainability, and early incorporation of AI into the cybersecurity lifecycle.
- Future research should focus on human-AI collaboration, resilience against adversarial attacks, and cross-disciplinary techniques.
- Future development of AI should address new threats, scalability, deployment issues, and organizational preparedness.

AI System Vulnerabilities to Cyberattacks: A Comprehensive Analysis

- AI system vulnerabilities to cyberattacks are classified into manipulation attacks and extraction assaults.
- Techniques used include machine learning (ML), deep learning (DL), and defense mechanisms like adversarial training, feature squeezing, and robust aggregation approaches.
- The study describes various types of attacks, including adversarial attacks, poisoning attacks, model inversion, and extraction attacks.
- A comparative analysis of major studies in AI and cybersecurity is conducted, highlighting the unique methods and results of each study.

AI and Machine Learning in Cybersecurity: A Comprehensive Review

- AI is used in intrusion detection, malware detection, and network security.
- Unsupervised learning methods are used to detect new dangers.
- Applications include security automation, threat intelligence, vulnerability management, and security education.
- The most important categories include asset management, threat hunting, vulnerability assessment, incident response, and dealing with malware, phishing, advanced persistent threats, and insider threats.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612055|

AI in Software Vulnerabilities and Malware

• AI can enhance malware detection and software security using techniques like data mining, machine learning classifiers, deep learning architectures, and metaheuristic algorithms.
• The Hybrid Metaheuristics Feature Selection with Stacked DL Enabled Cyber-Attack Detection (HMFS-SDLCAD) model is used to address cybersecurity in the Internet of Things (IoT) environment.

Current Malware Threats and Machine Learning

• Malware attacks are becoming more complex due to technology improvements and new exploitation techniques.
• The need for detection systems to constantly evolve is highlighted.
• Machine learning methods are becoming popular to fight against the rapid development of malware.
• An et al. revolutionized the field of cyber security by inventing a CNN-based model for automated vulnerability discovery.

VII. CONCLUSION

Artificial intelligence (AI) has had a tremendous influence on everyday life and business by allowing computers to execute activities that previously needed human intelligence. AI systems excel in real-time data analysis and decision-making, making them invaluable in cybersecurity. However, the complexities of threats, especially those based on AI, are always evolving. Even if employing professionals is expensive, AI may dramatically cut the costs and time needed for threat detection algorithms. AI can detect changes in attack trends, manage enormous volumes of data, and improve threat response. However, using AI in cybersecurity is difficult because of the vast quantity of data necessary, the possibility of false warnings, and the latency in responding to attacks. Despite these obstacles, current research is boosting AI's capacity to resist cyberattacks. A overview of AI approaches, such as machine learning, deep learning, and metaheuristic algorithms, covers a wide range of cyber risks, including malware, network intrusions, insider threats, botnets, and spam. Future proposals include continuous progress, the creation of new datasets, transparency, explainability, and the early integration of AI into the cybersecurity lifecycle for preventive actions. Future research should prioritise human-AI cooperation, robustness to adversarial threats, and cross-disciplinary approaches.

The research provides a complete examination of AI system vulnerabilities to cyberattacks, categorising them as manipulation attacks and extraction assaults. The work employs ML, DL, and defence mechanisms such as adversarial training, feature squeezing, and robust aggregation techniques. It covers a variety of methods, including adversarial assaults, poisoning attacks, model inversion, and extraction attacks. The paper also contrasts the present status of research in artificial intelligence and cybersecurity, emphasising each study's distinct techniques and findings.

The article examines the application of artificial intelligence in cybersecurity, specifically supervised learning for intrusion detection, malware detection, and network security. It also covers topics like security automation, threat intelligence, vulnerability management, and security education. The NIST framework-based study of AI applications in cybersecurity emphasises the relevance of automation, threat detection, and reaction accuracy.

Data mining, machine learning classifiers, deep learning architectures, and metaheuristic algorithms have all been utilised in research to improve detection and security of software flaws and viruses. The report also looks at how malware assaults are becoming more complicated and the necessity for detection systems to evolve over time. The authors also offer a CNN-based approach for automated vulnerability finding that uses deep learning to outperform traditional static analysis.

REFERENCES

1. AbuBakar, A., & Zolkipli, M. F. (2023). Cyber security threats and predictions: A survey. *International Journal of Advanced Engineering and Management (IJAEM), 5*(2), 733. https://doi.org/10.35629/5252-0502733741.
2. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics (Switzerland), 11*(1), 1–34. https://doi.org/10.3390/electronics11010016.
3. Alsamiri, J., & Alsubhi, K. (2019). Internet of things cyber attacks detection using machine learning. *International Journal of Advanced Computer Science and Applications, 10*(12), 627–634. https://doi.org/10.14569/ijacsa.2019.0101280.
4. Eswaran, M., et al. (2023). Survey of cyber security approaches for attack detection and prevention. *IEEE Access, 12*(1), 1–6. https://doi.org/10.17762/turcomat.v12i2.2406.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612055|

5. Morovat, K., & Panda, B. (2020). A survey of artificial intelligence in cybersecurity. *Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI 2020)* (pp. 109–115). https://doi.org/10.1109/CSCI51800.2020.00026.
6. Musa, N. S., Mirza, N. M., Rafique, S. H., Abdallah, A. M., & Murugan, T. (2024). Machine learning and deep learning techniques for distributed denial of service anomaly detection in software-defined networks—Current research solutions. *IEEE Access, 12*(January), 17982–18011. https://doi.org/10.1109/ACCESS.2024.3360868.
7. Parkar, P., & Bilimoria, A. (2021). A survey on cyber security IDS using ML methods. *Proceedings of the 5th International Conference on Intelligent Computing and Control Systems (ICICCS 2021)* (pp. 352–360). https://doi.org/10.1109/ICICCS51141.2021.9432210.
8. Perwej, Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, N., & Kumar Jaiswal, A. (2021). A systematic literature review on cyber security. *International Journal of Scientific Research and Management, 9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04.
9. Rauf, U., Mohsen, F., & Wei, Z. (2023). A taxonomic classification of insider threats: Existing techniques, future directions, and recommendations. *Journal of Cyber Security and Mobility, 12*(2), 221–252. https://doi.org/10.13052/jcsm2245-1439.1225.
10. Thanh, S. N., Stege, M., El-Habr, P. I., Bang, J., & Dragoni, N. (2021). Survey on botnets: Incentives, evolution, detection, and current trends. *Future Internet*. https://doi.org/10.3390/fi13080198.
11. Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security, 15*(5), 390–396. https://doi.org/10.6633/IJNS.201309.
12. Parizad, A., & Hatziadoniu, C. J. (2022). Cyber-attack detection using principal component analysis and noisy clustering algorithms: A collaborative machine learning-based framework. *IEEE Transactions on Smart Grid, 13*(6), 4848–4861. https://doi.org/10.1109/TSG.2022.3176311
13. *Philosophical logic and artificial intelligence*. (1989). Springer Netherlands. https://doi.org/10.1007/978-94-009-2448-2
14. Pomerol, J.-C. (1997). Artificial intelligence and human decision making. *European Journal of Operational Research, 99*(1), 3–25. https://doi.org/10.1016/S0377-2217(96)00378-5
15. Dokur, N. B. (n.d.). *Artificial Intelligence (AI) applications in cyber security*. ResearchGate. https://www.researchgate.net/publication/367253331
16. Hua, L. J. (2018). Cyber security meets artificial intelligence: A survey. *Frontiers of Information Technology & Electronic Engineering, 19*(12), 1462–1474. https://doi.org/10.1631/FITEE.1800573
17. Welukar, J. N., & Bajoria, G. P. (2021). Artificial intelligence in cyber security—A review. *International Journal of Scientific Research in Science and Technology*. https://doi.org/10.32628/IJSRST218675
18. Thomas, T., Vijayaraghavan, A. P., & Emmanuel, S. (2019). *Machine learning approaches in cyber security analytics*. Springer. https://doi.org/10.1007/978-981-15-1706-8
19. Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L., & Koyuncu, M. (2022). Cybersecurity deep: Approaches, attacks dataset, and comparative study. *Applied Artificial Intelligence*. https://doi.org/10.1080/08839514.2022.2055399
20. Nordin, N. S., et al. (2021). A comparative analysis of metaheuristic algorithms in fuzzy modelling for phishing attack detection. *Indonesian Journal of Electrical Engineering and Computer Science, 23*(2), 1146–1158. https://doi.org/10.11591/ijeecs.v23.i2.pp1146-1158
21. Agrawal, P., Abutarboush, H. F., Ganesh, T., & Mohamed, A. W. (2021). Metaheuristic algorithms on feature selection: A survey of one decade of research (2009–2019). *IEEE Access, 9*, 26766–26791. https://doi.org/10.1109/ACCESS.2021.3056407
22. Kuntla, G. S., Tian, X., & Li, Z. (2021). Security and privacy in machine learning: A survey. *Issues in Information Systems, 22*(3), 224–240. https://doi.org/10.48009/3_iis_2021_242-258
23. Peng, J., Jury, E. C., Dönnes, P., & Ciurtin, C. (2021). Machine learning techniques for personalised medicine approaches in immune-mediated chronic inflammatory diseases: Applications and challenges. *Frontiers in Pharmacology, 12*, 1–18. https://doi.org/10.3389/fphar.2021.720694
24. Alduailij, M., Khan, Q. W., Tahir, M., Sardaraz, M., Alduailij, M., & Malik, F. (2022). Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method. *Symmetry, 14*(6), 1–15. https://doi.org/10.3390/sym14061095
25. Gawand, M. K. S. P. (2013). *A comparative study of cyber attack detection & prediction using machine learning algorithms*. ResearchGate. https://doi.org/10.21203/rs.3.rs-3238552/v1
26. Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet of Things, 14*, 100393. https://doi.org/10.1016/j.iot.2021.100393
27. Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things, 7*, 100059. https://doi.org/10.1016/j.iot.2019.100059

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612055|

28. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*. https://doi.org/10.1186/s40537-020-00318-5
29. Rodriguez, E., Otero, B., Gutierrez, N., & Canal, R. (2021). A survey of deep learning techniques for cybersecurity in mobile networks. *IEEE Communications Surveys & Tutorials, 23*(3), 1920–1955. https://doi.org/10.1109/COMST.2021.3086296
30. Pourafshin, F. (2021). Big data mining in internet of things using fusion of deep features. *International Journal of Scientific Research in Engineering Trends, 7*(2), 1089–1093.
31. Gu, H., Wang, Y., Hong, S., & Gui, G. (2019). Blind channel identification aided generalized automatic modulation recognition based on deep learning. *IEEE Access, 7*, 110722–110729. https://doi.org/10.1109/ACCESS.2019.2934354
32. Hassan, I. H., Mohammed, A., & Masama, M. A. (2023). Metaheuristic algorithms in network intrusion detection. In *Comprehensive metaheuristics* (pp. 95–129). Elsevier. https://doi.org/10.1016/B978-0-323-91781-0.00006-5
33. Rajwar, K., Deep, K., & Das, S. (2023). An exhaustive review of the metaheuristic algorithms for search and optimization: Taxonomy, applications, and open challenges. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-023-10470-y
34. Role of AI in cyber security through anomaly detection and predictive analysis. (2023). *Journal of Information and Education Research, 3*(2). https://doi.org/10.52783/jier.v3i2.314
35. Ozkan-Okay, M., et al. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEE Access, 12*, 12229–12256. https://doi.org/10.1109/ACCESS.2024.3355547
36. Sangwan, R. S., Badr, Y., & Srinivasan, S. M. (2023). Cybersecurity for AI systems: A survey. *Journal of Cybersecurity and Privacy, 3*(2), 166–190. https://doi.org/10.3390/jcp3020010
37. Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*. https://doi.org/10.1080/23311916.2023.2272358
38. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*. https://doi.org/10.1016/j.inffus.2023.101804
39. Bin Hulayyil, S., Li, S., & Xu, L. (2023). Machine-learning-based vulnerability detection and classification in internet of things device security. *Electronics, 12*(18), 3927. https://doi.org/10.3390/electronics12183927
40. Asiri, M. M., et al. (2023). Hybrid metaheuristics feature selection with stacked deep learning-enabled cyber-attack detection model. *Computer Systems Science and Engineering, 45*(2), 1679–1694. https://doi.org/10.32604/csse.2023.031063
41. Caviglione, L., et al. (2021). Tight arms race: Overview of current malware threats and trends in their detection. *IEEE Access, 9*, 5371–5396. https://doi.org/10.1109/ACCESS.2020.3048319
42. An, J. H., Wang, Z., & Joe, I. (2023). A CNN-based automatic vulnerability detection. *EURASIP Journal on Wireless Communications and Networking*. https://doi.org/10.1186/s13638-023-02255-2
43. Lucky, G., Jjunju, F., & Marshall, A. (2020). A lightweight decision-tree algorithm for detecting DDoS flooding attacks. In *Proceedings—Companion of the 2020 IEEE 20th International Conference on Software Quality, Reliability, and Security (QRS-C)* (pp. 382–389). IEEE. https://doi.org/10.1109/QRS-C51114.2020.00072
44. Mynuddin, M., Hossain, M. I., Uddin Khan, S., Islam, M. A., Mohammed Abdul Ahad, D., & Tanvir, M. S. (2023). Cyber security system using fuzzy logic. In *2023 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*. IEEE. https://doi.org/10.1109/ICECCME57830.2023.10252778

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com