Plag Report

by Atul Sharma

Submission date: 29-Apr-2024 03:16PM (UTC+0530)
Submission ID: 2364345739
File name: Enhancing_Cybersecurity_Through_Automated_Vulnerability_Assessment.pdf (352.5K)
Word count: 4310
Character count: 26241

Enhancing Cybersecurity Through Automated Vulnerability Assessment: A Comprehensive Study on Integrating Machine Learning Models with Existing Tools

Abstract:

Robust automated vulnerability detection is crucial, as evidenced by the growing complexity and interconnectivity of contemporary software systems. It is concerning how software vulnerabilities affect frequently used software systems. With so many variables to take into account, patching and service reliability have to be balanced, and there are a lot of vulnerabilities to address, choosing remediation strategies is a difficult task in the IT business. Remedial choices are now taken manually, which is unfortunately time-consuming. This raises the danger to security and drives up the expense of vulnerability control. Software vulnerability identification is still a major problem, despite the many deep learning-based models that have been developed to automate ulnerability detectio

The adoption of artificial intelligence methodologies, especially Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL), has become crucial in the field of cybersecurity because of the steadily increasing frequency of assaults. These methods have shown to be successful in identifying and averting cyberattacks, which have the potential to serious risks to people, companies, and even nations. Security researchers may now spot risks and vulnerabilities that were previously unknown to them thanks to machine learning algorithms that employ statistical techniques to find correlations and abnormalities in massive datasets.

he purpose of this paper is to create an automated vulnerability detection tool based on machine learning. We want to solve the shortcomings of current tools and provide the groundwork for the creation of more dependable vulnerability assessment systems by evaluating deep learning-based techniques.

Additionally, the paper discusses the challenges associated with automated vulnerability assessment, such as false positives, scalability, and evolving attack vectors. Finally, it proposes future research directions aimed at addressing these challenges and advancing the field of automated vulnerability assessment.

Keywords: **Vulnerability, Patching, Deep learning, Security, Automated, Detection, Static Analysis, Dynamic Analysis, Hybrid Approaches, Threat Detection, False Positives.**

I. Introduction:

These days, information systems permeate practically every aspect of life and the dependability, security, and safety of software applications are essential to nearly every business. Each aspect of our lives is enhanced by technology, which offers us numerous benefits but also presents some challenges. The growing hazards to cyber security as the consequence of daily technological advancements is one of these issues [1][2]. Thus, to keep the program from being compromised, it is imperative that you recognize and fix code that has known vulnerabilities. Since practically every gadget in use today has an Internet connection, cybernetic attacks represent a genuine threat to businesses and individuals in general. Devices are thus vulnerable to outside attacks that aim to take advantage of weaknesses. As is evident from various studies, cybercrime has harmed several organizations, companies, and individuals in recent years. Financial documents, personal information, and confidential intelligence data are l among the stolen materials. By the end of 2023, more than 1.8 million cyber security personnel will be required, according to research on the effects of cyber security on businesses and individuals. Additionally, it is claimed that businesses would invest at least $100 billion annually on cyber security defense [3], [4], [5].

The rapid expansion of software development has brought about unprecedented technological advancements but has also heightened cyber risks. As organizations harness networked systems and applications, software vulnerabilities become potential entry points for malicious actors and the ever-expanding area of software development has brought about an age of unmatched technical advancement, but it has also brought about an equally incredible surge in cyber risks. As organizations endeavor to harness the power of networked systems and applications, software vulnerabilities become potential ports of entry for

hostile actors. Traditional static analysis techniques, while useful, may fall short of addressing complex vulnerabilities effectively, often yielding high rates of false positives and negatives. A lot of these ideas are provided during any software development process because practically every aspect of our society involves electronic devices that run the software, making it necessary to either completely eradicate or greatly reduce the likelihood of events that could jeopardize the security of data or operations. Even if they are useful, the conventional techniques of static analysis are not sufficient for addressing complex patterns and subtle weaknesses in software code. Vulnerabilities come in a variety of forms and are categorized according to several factors. They make available vulnerabilities, attacks, and fixes that have been found in online databases. Exploits continue to happen despite the abundance of sources and knowledge regarding vulnerabilities.

Software vulnerability and Deep Learning are the primary sources of inspiration for the research presented in this article and the efforts of experts worldwide. To comprehend all of the approaches that will be discussed in the following sections, one must have a solid understanding of the concepts of vulnerability, deep learning, and other related ideas. A vulnerability is characterized as an imperfection or weakness that might be used to circumvent the security policy of the system in the system's operation, administration, or implementation (the way the algorithms are implemented in the selected programming languages) [6]. These defects might be in the creation, design, or operation of the system, and their exploitation could have negative effects. Normally, this viewpoint of damage or information loss is referred to as risk.

Let me introduce deep learning, a paradigm-shifting approach that has proven very effective in identifying intricate patterns and correlations within large-scale datasets. To transform automated vulnerability detection systems, this project investigates the integration of deep learning. A type of machine learning known as deep learning has changed the game in several fields, and its use in cybersecurity promises to improve the precision and effectiveness of risk assessments. Deep learning algorithms demonstrated a tendency to find tiny patterns that conventional methods would miss. Combining automated vulnerability detection tools like Nessus and OpenVas with deep learning not only solves the shortcomings of current solutions but also ushers in a new age of proactive cybersecurity. Organizations may strengthen their defenses against cyber-attacks by utilizing neural network capabilities, which can detect vulnerabilities more precisely and decrease the probability of false alarms.

Modern software programs are large and sophisticated, which frequently results in missed security flaws and programming faults. Studies have indicated that over half of a developer's time is dedicated to finding and resolving issues [7], [8]. In actuality, they often audit the code and search for security flaws using automated program analysis or testing techniques. A strong analytic tool can identify and eliminate vulnerabilities; moreover, it is increasingly being incorporated into the development process. However, there is always an opportunity for improvement, and all of the research being done in this field has the potential to be extremely valuable to the business. The purpose of this study is to investigate how well deep learning-based methods work for automating the detection of software vulnerabilities. We want to explore the possible benefits that deep learning brings to the forefront of cybersecurity through a comparative examination with classic static analysis methods. The use of machine learning models is anticipated to be a fundamental component in fortifying organizations' defenses against cyber-attacks as they moreover through the always-changing environment of threats.

1.2MACHINE LEARNING KEY Challenges FOR CYBERSECURITY

While machine learning techniques help resolve cybersecurity-related concerns, they are not infallible in all cases. These difficulties can be summed up as follows:

- Data speculating
- False Positive
- Enormous volume of data
- High Dimensional
- Challenging to recognize and protect data from unidentified risks.
- Data preparation is a hurdle.
- Relevant elements are vital since the flows contain inadequate information.

1.2 Research Questions (RQ)

RQ1: How do alternative models of artificial intelligence and machine learning assist in handling cyber-related issues?

RQ2: Exactly how effective are AI and ML methods in addressing the continually developing Cybersecurity landscape?

RQ3: How can machine learning and artificial intelligence techniques generalize across numerous datasets?

RQ4: The extent to which cybersecurity decision-making by AI and ML models can be explained, and how does this impact the models' acceptability?

RQ5: How are big data sets and complicated data handled by AI and ML?

1.3 Benefits to using ML in cybersecurity [9], [10], [11], [12], [13]:

- Enhanced accuracy: Large data sets may be analysed by machine learning algorithms, which can also identify intricate patterns that can be hard for human analysts to identify. With this feature, there may be fewer false positives and a greater degree of precision in identifying potential threats.
- Quick detection: Identification and mitigation of potential dangers may happen more quickly when real-time data analysis is done with machine learning techniques.
- Automation: Human analysts may focus on more complex tasks by applying machine learning algorithms to automate time-consuming tasks associated with threat detection and response.
- Scalability: Because ML algorithms can scale to analyze enormous amounts of data, they are well-suited for large-scale cybersecurity operations.

II. Importance of Vulnerability Assessment

Protecting the confidentiality, availability, and integrity (CIA) [d2] of user and organisational private data requires regular vulnerability assessments. Regularly identifying and fixing security flaws helps prevent data theft, alteration, and disclosure while also preventing corporate activities from being disrupted. According to the research, the overall financial losses resulting from the assault, both direct and indirect, are typically found to be more than the expenses associated with purchasing data protection systems and making regular investments in security technology [d3]. In a similar vein, other research [14, 15] also shows that identifying the most important assets and regularly evaluating their vulnerabilities can help shield the company from significant financial losses. A data breach frequently results in significant expenses for the company, such as those associated with determining the cause of the assault, retrieving and repairing lost data, alerting customers, setting up hotlines, and covering settlements and legal fees [16]. When a cyberattack compromises a customer's data or private information, the affected firm frequently faces negative publicity and defamation. For instance, a ransomware assault on the National Health Service in the UK in 2017 brought up several concerns over the security posture of vital IT systems that are widely relied upon by users.
Additionally, it has been demonstrated that software systems are essentially defective because of purposeful or unintentional flaws and that even a small number of these flaws may be leveraged to obtain complete access and result in significant harm [17]. These problems have the potential to seriously harm a firm by losing customers, among other things. One survey found that when a breach occurs, there is often an instantaneous loss of 11% of the customer base. This can be mitigated, though, if consumers are promptly notified of the next actions they need to take and are encouraged by the offer of settlements.

2.1 Techniques of detection

The ubiquitous problem of vulnerabilities in software development has led to the creation of several approaches to deal with the problem, one of them being in-depth code audits. Defensive programming is a solid strategy that emphasizes anticipating potential security vulnerabilities when coding, although it is not a perfect solution for all

vulnerability-related difficulties [18]. Because certain libraries, programming languages, or APIs were not created with security considerations in mind, it might be difficult even for experienced programmers to anticipate every possible exploit. Alternative strategies have been devised and implemented in response to the realization that good intentions and behaviors by themselves are inadequate to address vulnerabilities. Several methods are examined in this section, all of which are meant to help reduce software vulnerabilities:

- **Static Analysis for Security Testing (SAST):** Static analysis techniques are used in Security Testing (SAST) as automated tools to find logical, safety, and security flaws in software systems. By automating the identification process and doing away with the necessity for laborious manual code checks, these technologies are extremely helpful in saving time and resources .
- **Dynamic Analysis for Security Testing (DAST):** DAST approaches vulnerability identification from a testing-centric perspective. Using this approach, the security of a programme is assessed and tested in real-time. DAST tools or testers engage with the programme as external users, ignorant of its internal workings, treating the tested software as a "black box."
- **Interactive Analysis for Security Testing (IAST):** IAST sets itself apart by sharing SAST's goal of using internal analysis to find vulnerabilities. But like DAST, IAST analyzes while the program is operating**,** offering a hybrid method that combines the benefits of dynamic and static analysis.

2.2 Machine Learning in Vulnerability Identification:

As a result of the resource-intensive nature and limits of current vulnerability assessment tools, there has been an increase in interest in using machine learning, particularly deep learning, to automate operations across a variety of areas. Machine learning has shown promise in fields such as picture identification and illness prediction. To address the drawbacks of conventional techniques, machine learning has become popular in the field of software security to identify vulnerabilities. This research focuses on investigating and assessing the efficacy of machine learning, especially deep learning, as a revolutionary force in automated vulnerability detection systems as we traverse the complex terrain of vulnerability identification. The nuances of these methods and how they might be used to strengthen software against possible cyberattacks will be covered in detail in the following sections. These examples illustrate the diversity of approaches in integrating machine learning with vulnerability assessment tools, each with its own set of advantages and challenges. The proposed system, DeepNessus, aims to address some of these challenges by leveraging the capabilities of both Nessus and deep learning techniques

Related Work	Description	Pros	Cons
DeepNessus (Proposed System)	Integrates Nessus with deep learning models	- Utilizes Nessus' extensive vulnerability database - Enhances accuracy and speed of vulnerability detection	- Requires significant computational resources - Complexity in training and maintenance
AutoVulnScan	Uses machine learning for vulnerability assessment	- Automation of vulnerability scanning tasks - Improved detection of complex vulnerabilities	- Limited to specific types of vulnerabilities - Dependency on labeled datasets
VULCON	Combines vulnerability data with ML algorithms	- Provides real-time vulnerability assessment - Adapts to evolving threats	- Limited scalability for large-scale networks - May produce false positives/negatives
ML-Vuln-Scanner	Applies ML techniques to enhance vulnerability scanning	- Detects previously unknown vulnerabilities - Reduces false positive rates	- Requires continuous updating of ML models - Complexity in integrating with existing tools

III. Related work :

Study	Integration Approach	Pros	Cons
Using Machine Learning for Vulnerability Detection and Classification[19]	Automatic vulnerability identification and classification in source code	- Improves efficiency and accuracy of vulnerability detection - Provides insights into specific vulnerability types	- Requires access to large codebases for training - May not be effective for complex or obfuscated code
Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners[20]	Aggregates result from multiple vulnerability scanners (WAVS) using an automation and combination algorithm	- Improves detection rate by combining results from different tools - Reduces redundancy in vulnerability reports	- Requires development and maintenance of the integration framework - May not address zero-day vulnerabilities
Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification[21]	Analyzes network traffic and code for threat patterns using machine learning	- Expedites threat detection and analysis - Improves accuracy of forensic investigations	- Requires large datasets for training ML models - May be susceptible to adversarial attacks
Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects[22]	Analyzes various cybersecurity data using various ML techniques	- Provides insights from vast amounts of data - Enables proactive security measures	- Requires expertise in both cybersecurity and ML - Scalability can be an issue
Detection of Vulnerability Scanning Attacks using Machine Learning[23]	Identifying malicious scanning attempts disguised as vulnerability scans	- Reduces false positives from vulnerability scans - Prioritizes security	- Requires labeled data for training, which can be limited - May need continuous

		responses for real threats	adaptation as attack techniques evolve
A Survey on Machine Learning for Software Vulnerability Analysis [24]	Broad overview of ML approaches for software vulnerability analysis (detection, prioritization, patching)	- Comprehensive analysis of various ML techniques - Explores potential for proactive security measures	- Requires expertise in both cybersecurity and ML - Scalability challenges for large software systems
Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security[25]	Detecting vulnerabilities in Internet of Things (IoT) devices	- Tailored approach for vulnerabilities specific to IoT devices - Automates vulnerability detection for large numbers of devices	- Limited research on applying ML to diverse IoT ecosystems - Data security and privacy concerns for IoT device data

IV. Proposed System

Through a smooth integration of machine learning capabilities with current tools such as Nessus, our proposed solution seeks to transform vulnerability assessment. The architecture is made up of several interrelated parts, each of which is essential to improving security assessments and automating vulnerability identification. Our system's initial phase is to collect vulnerability data from a variety of sources, such as publicly accessible datasets and repositories. This data includes critical characteristics including vulnerability numbers, descriptions, and related properties. We download the national dataset consisting of all the vulnerabilities with the CVE number, description, Severity level, etc. Before feeding the data into our machine learning model, we undergo a meticulous preprocessing phase. To manage missing values, eliminate inconsistencies, and encode category variables, we clean the data in this section. To make sure the dataset is suitable for efficient model training, this preliminary step is really important.

After Preprocessing the dataset we Utilize TensorFlow as our foundation, we create an ML model specifically for flaw diagnosis by using a custom-made neural network. Although this model is designed to discover deeply embedded semiotic openings and markers from data, it goes back further to the information security sphere and aims to embrace and encourage knowledge beyond the classical information security methods. Via a repeated mode of learning, the model mastery in vetting a correct classification of vulnerabilities against descriptions and other relevant data. Then, there comes model training in which propagated to these measures that are used, with accuracy, precision, recall rate, and F1-score as the main ones. This in-depth assessment lets us check whether our model is capable of revealing vulnerabilities in high precision with reliability such that detection is maximum. Once the model is

trained we save the model with the .kerbos for further use. The centerpiece of our system is its flawless combination with well-known vulnerability assessment tools e.g. Nessus. The system lets the user configure the alerts regardless of the vulnerability level. We achieve this by building the NASL scripts that interact well with our already manufactured machine-learning models and integrating them into the Nessus framework. The scripts provide an option for automatic vulnerability detection through the predictions produced by that model. The ability of our system to put together the machine learning capabilities and the power of Nessus serves the security testing processes better by both enhancing effectiveness and efficiency.

V. CONCLUSION

In the linked world of today, cybersecurity is more important than ever. As cyberattacks and data breaches become more common, people and organizations are in danger from malevolent actors. Therefore, it is essential to take preventative action to shield digital assets from those dangers. Increasing knowledge and education is one of the best strategies to strengthen cybersecurity. People may reduce their chance of becoming victims of cyberattacks by keeping up to date on the most recent dangers and best practices. Organizations must prioritize cybersecurity in addition to individual efforts to safeguard their networks and data. Recognizing and addressing any risks entails putting strong security processes into place and making investments in cutting-edge technology like artificial intelligence and machine learning. This paper thoroughly examines emerging technologies, their contributions to cybersecurity, and both their benefits and drawbacks. Despite the abundance of research on machine learning (ML) in cybersecurity, there isn't a current study that goes into detail on ML, DL, or RL. The researchers will use this study as a guide to highlight the role, methods, and significance of machine learning in the cybersecurity domain.

ML is a potent instrument that may be used to enhance cybersecurity. ML algorithms may assist organizations in real-time threat identification and response by analyzing massive datasets and detecting trends in network behavior. This can strengthen an organization's overall security posture and allow for quicker and more efficient responses to threats. Although machine learning (ML) has shown a lot of promise for enhancing cybersecurity, there remain obstacles to overcome in its use.

VI. Results

The performance of the planned system for assessing vulnerabilities automatically and precisely turned out to be reassuring both in respect of multiple evaluation areas. By engaging in a systematic data collection and preprocessing movement, our different data attributes covering various aspects of vulnerability were put together to come up with a complete dataset. This set of data has been regarded as a base, which has been used to simplify the task of a neural network model which employs TensorFlow within the mining process of patterns and characteristics of vulnerability data.

After training and evaluating the given model, it was noticeable that our proposed method led to accuracy enhancements in vulnerability detection which exceed those obtained through traditional means. The model drew a satisfactory result on the different metrics' such as accuracy, precision, recall and F1 score. As the result, the interaction with Nessus was the key to overall automation of vulnerabilities spotting process which had a positive impact on efficacy and efficiency of security evaluation performance.

The combination of experiments with real-world scenarios and case studies provide evidence that our approach to identifying and mitigating vulnerability is done on time and preventive. Analyzing the numbers, organizations that powered the system noticeably reduced the time for vulnerability assessment compared to previous time, so, they could lessen the lifespan of reportedly known security risks and encounter cyber threats less often.

REFERENCES

[1] K. Thakur, M. Qiu, K. Gai, and M. L. Ali, "An investigation on cyber security threats and security models," in Proc. IEEE 2nd Int. Conf. Cyber Secur. Cloud Comput., Nov. 2015, pp. 307–311.

[2] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," Energy Rep., vol. 7, pp. 8176–8186, Nov. 2021.

[3] M. Näsi, A. Oksanen, T. Keipi, and P. Räsänen, "Cybercrime victimization among young people: A multi-nation study," J. Scandin. Stud. Criminal. Crime Prevention, vol. 16, no. 2, pp. 203–210, Jul. 2015.

[4] S. van de Weijer, R. Leukfeldt, and S. Van der Zee, "Reporting cybercrime victimization: Determinants,

motives, and previous experiences,'' Policing, Int. J., vol. 43, no. 1, pp. 17–34, Mar. 2020.
[5] R. Searle and K. Renaud, "Trust and vulnerability in the cybersecurity context," in Proc. HICSS, 2023, pp. 5228–5240.
[6] Benjamin Steenhoek, Md Mahbubur Rahman, Richard Jiles, and Wei Le. 2023. An empirical study of deep learning models for vulnerability detection. In 2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE).
[7] "Today's state of vulnerability response: Patch work demands attention," https://www.servicenow.com/content/dam/servicenow/documents/analystresearch/ponemon-state-of-vulnerability-response.pdf, 2018.
[8] Guru Bhandari, Amara Naseer, and Leon Moonen. 2021. CVEfixes: automated collection of vulnerabilities and their fixes from open-source software. In Proceedings of the 17th International Conference on Predictive Models and Data Analytics in Software Engineering. 30–39.
[9] O. Yavanoglu and M. Aydos, "A review on cyber security datasets for machine learning algorithms," in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2017, pp. 2186–2193.
[10] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, Machine Learning Approaches in Cyber Security Analytics. Cham, Switzerland: Springer, 2020.
[11] I. H. Sarker, "Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective," Social Netw. Comput. Sci., vol. 2, no. 3, p. 154, May 2021.
[12] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018.
[13] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.
[14] Colin Raffel, Noam Shazeer, Adam Roberts, Katherine Lee, Sharan Narang, Michael Matena, Yanqi Zhou, Wei Li, and Peter J Liu. 2020. Exploring the limits of transfer learning with a unified text-to-text transformer. The Journal of Machine Learning Research 21, 1 (2020), 5485–5551.
[15] Chandra Thapa, Seung Ick Jang, Muhammad Ejaz Ahmed, Seyit Camtepe, Josef Pieprzyk, and Surya Nepal. 2022. Transformer-Based Language Models for Software Vulnerability Detection. In Proceedings of the 38th Annual Computer Security Applications Conference. 481–496.
[16] Xinda Wang, Shu Wang, Pengbin Feng, Kun Sun, and Sushil Jajodia. 2021. Patchdb: A large-scale security patch dataset. In 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 149–160.
[17] Yue Wang, Weishi Wang, Shafiq Joty, and Steven CH Hoi. 2021. Codet5: Identifier-aware unified pre-trained encoder-decoder models for code understanding and generation. arXiv preprint arXiv:2109.00859 (2021)
[18] Alexis Challande, Robin David, and Guénaël Renault. 2022. Building a Commitlevel Dataset of Real-world Vulnerabilities. In Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy. 101–106.
[19] A Drop of Knowledge Base for Vulnerability Detection and Classification (DROPS): https://arxiv.org/pdf/2310.18347
[20] M. Garcia et al., "Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners," Sensors (MDPI), vol. 12, no. 11, Art. no. 17334, Nov. 2022 DOI: 10.3390/s121117334: [Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners - MDPI study on vulnerability assessment]
[21] International Institute of Engineers and Technologists (IIETA), "Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification," https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.130412
[22] Iqbal H. Sarker et al., "Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects," Annals of Data Science, vol. 9, no. 1, pp. 77–108, 2022 DOI: 10.1007/s40745-022-00444-2: [Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects | Annals of Data Science - SpringerLink]
[23] kth.diva-portal.org
[24] A Survey on Machine Learning for Software Vulnerability Analysis - ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0167404820300353
[25] Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security - MDPI: https://www.mdpi.com/2079-9292/12/18/3927

Plag Report

ORIGINALITY REPORT

7%	%	6%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Merve Ozkan-Okay, Erdal Akin, ÖMER Aslan, Selahattin Kosunalp, Teodor Iliev, Ivaylo Stoyanov, Ivan Beloev. "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions", IEEE Access, 2024 Publication	3%
2	Bandr Fakiha. "Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification", International Journal of Safety and Security Engineering, 2023 Publication	1%
3	Submitted to Bahrain Polytechnic Student Paper	1%
4	Ateen Dubey, Geetika Tiwari, Anshika Dixit, Ananya Mishra, Mohit Pandey. "Chapter 49 Leveraging Innovative Technologies for Ransomware Prevention in Healthcare: A	<1%

Case Study of AIIMS and Beyond", Springer Science and Business Media LLC, 2024
Publication

5	Submitted to De Montfort University Student Paper	<1 %
6	Submitted to Ravensbourne Student Paper	<1 %
7	Franciskus Antonius, J.C. Sekhar, Vuda Sreenivasa Rao, Rahul Pradhan et al. "Unleashing the power of Bat optimized CNN-BiLSTM model for advanced network anomaly detection: Enhancing security and performance in IoT environments", Alexandria Engineering Journal, 2023 Publication	<1 %
8	Gonaygunta, Hari. "Factors Influencing the Adoption of Machine Learning Algorithms to Detect Cyber Threats in the Banking Industry", University of the Cumberlands, 2024 Publication	<1 %
9	Rongcun Wang, Senlei Xu, Xingyu Ji, Yuan Tian, Lina Gong, Ke Wang. "An extensive study of the effects of different deep learning models on code vulnerability detection in Python code", Automated Software Engineering, 2024 Publication	<1 %

10	Ton Duc Thang University Publication	<1%
11	Yizheng Chen, Zhoujie Ding, Lamya Alowain, Xinyun Chen, David Wagner. "DiverseVul: A New Vulnerable Source Code Dataset for Deep Learning Based Vulnerability Detection", Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses, 2023 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		