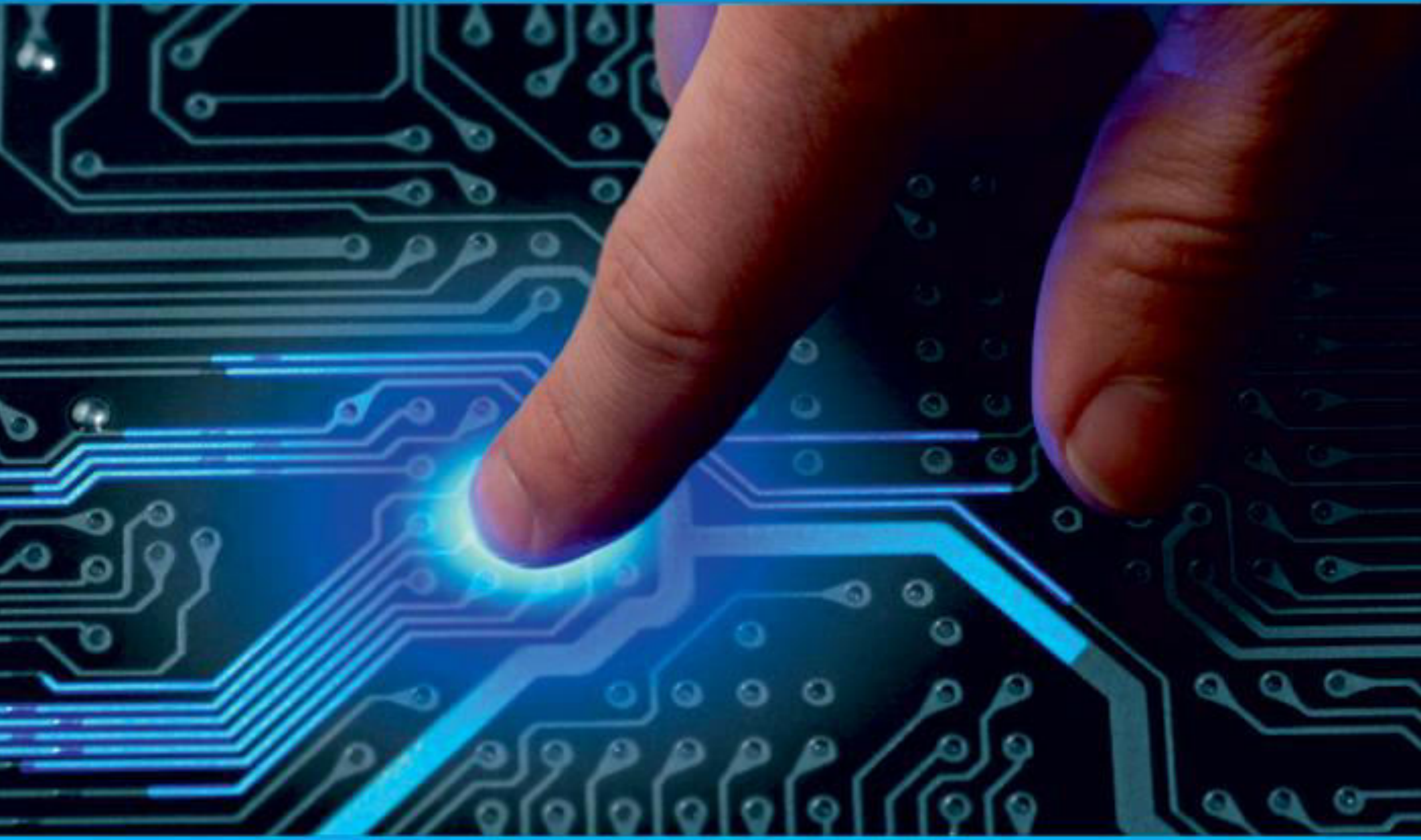
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 8, August 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.625

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Beyond Manual Testing: How AI is Revolutionizing Performance & Security

Priya Yesare

Principal SQA Engineer, Asurion, Nashville, Tennessee, USA

ABSTRACT: The paper examines how AI can improve performance and security testing, increasing response time, throughput, and accuracy of threat detection. The experimental results demonstrate that there is a 26.2% improvement in the throughput time, an 31.2% increase in the throughput, and 95%+ threat detection accuracy. Real time optimization is provided by AI based testing that eliminates vulnerabilities faster and make the system more reliable and efficient.

KEYWORDS: AI, Test, Performance, Security

I. INTRODUCTION

Scaling up for traditional software testing is also challenging, along with detecting real time threats. Performing this task using AI-pushed testing automates the process of performance optimization as well as threat identification. This research presents the uses of the artificial intelligence in mitigating cyber threats, detection of bottlenecks and improvement in throughput. By showing our findings, we illustrate the way in which AI can replace the conventional software testing to realize mass and robust, adaptive systems.

II. RELATED WORKS

2.1 Predictive Analytics

AI’s role in the performance testing is coming into limelight because AI can predict system failure and optimize the system before the system bottleneck affects the user. Predictive analytics supported by AI use historical data and various machine learning (ML) methods to find signs of a performance downfall (Grzonka et al., 2018).

Unlike traditional monitoring systems where the resource monitoring and alerting runs only after the incident happens, AI models can actively adjust the resource to ensure resource balance would be optimized in real time. In large scale distributed environments like cloud computing, such systems can be created using multi agent framework to ensure that they are highly reliable (Grzonka et al., 2018).

Anomaly detection using the AI is crucial to mitigate the performance issues on the complex systems, Internet of Things (IoT) network for example. In an AI based testbed architecture (Moustafa, 2021), it was presented that cyber threats are evaluated in IoT networks.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

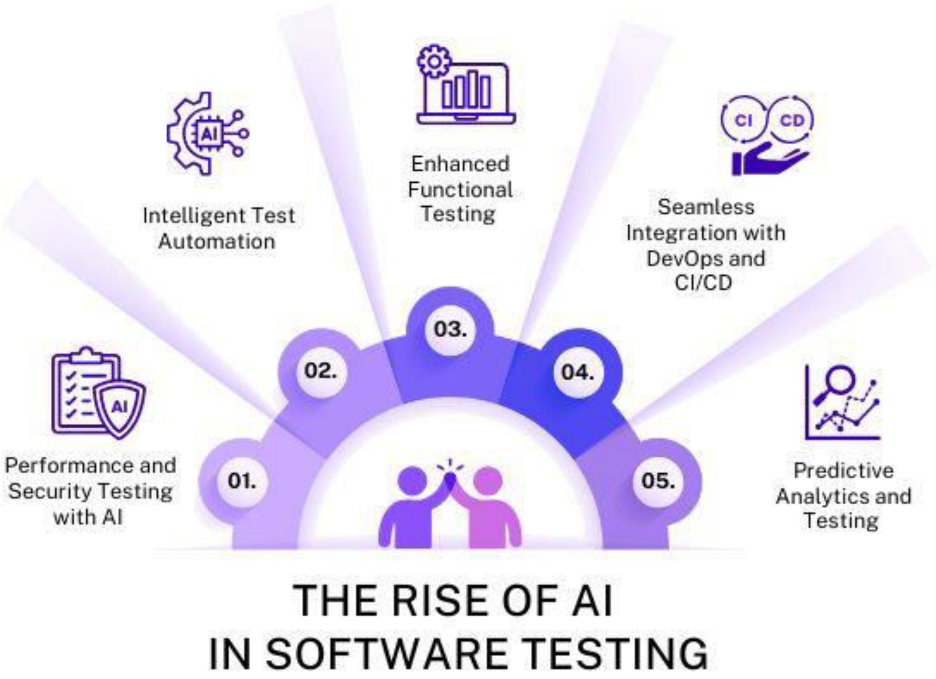

Intelligent Test Automation
Enhanced Functional Testing
CI
CD
Seamless Integration with DevOps and CI/CD
Performance and Security Testing with AI
AI
01.
02.
03.
04.
05.
Predictive Analytics and Testing
THE RISE OF AI IN SOFTWARE TESTING

Figure 1 Software Testing (BugRaptors, 2023)

The collected data from this platform is heterogeneous data sourced from IoT services, with predicted and detected anomalies created by ML algorithms like Gradient Boosting Machines and Deep Neural Networks.

Similarly, Meziane & Ouerdi (2023) studied a variety of the IoT security AI techniques viz. ML and Deep Learning (DL) to decide maximum classification accuracy. The results indicate that AI driven anomaly solution can substantially improve its performance by monitoring the system behaviour and predicting failures prior to turning into critical failures.

In addition, AI provides great efficiency in evaluating real time data performance of complex environments: integrated circuits (ICs). Akter et al. (2021) develop a non-destructive AI based terahertz testing method for the detection of defective ICs.

Using convolutional neural networks (CNN), this method is applied to terahertz radiation responses in order to classify faulty components with an accuracy rate of 94%. Different perspectives based on the external and internal relationship of teams and systems, respectively, predictively using the above-mentioned AI driven approaches are shedding the light over the potential of predictive analytics for reduced incidence of system failures and better performance optimization in a myriad of applications.

2.2 Vulnerability Detection

As the sophistication of cyber threats has been growing, AI-based pen testing has evolved to be a powerful means to automate the vulnerability detection on software systems. However, the traditional penetration testing is based on manual effort and predefined test cases which are less adaptive in the dynamic security risk elements (Bozic & Wotawa, 2017).

ML driven penetration testing uses ML algorithms to automate pen testing process, identifying security flaws dynamically by behaviours in a scenario close to the one of the real attacks. Azar et al. (2022) highlights the importance of AI in verifying security for system on chips (SoC), which are highly at risk to unauthorized access and malicious attack.

The ability to self-refine with modern electronic design automation (EDA) tools, the study showed, had penetration testing tools made available via AI. Unlike traditional approaches, AI based test case refinement can change future threats, adapt to them and increase detection accuracy.

AI penetration testing is equally important to detect vulnerability in ‘software applications’ other than SoCs. In his paper, Bakhshandeh et.al (2023) applied AI tools for security code review and NLP techniques for automatic analysis and detection of security loopholes in codebases.

ChatGPT is an AI model whose power to suggest vulnerabilities and corrective actions in alignment with traditional static analysis tools has been shown to be strong. In addition, there has been use of AI based security solutions for buffer overflow detection and hardware security.

In this paper, Sestili et al. (2018) compare with static analysis tools in detecting buffer overflow vulnerabilities. According to their findings, AI derived based solutions need a lot of training datasets to reach the accuracy of static analysis engines, however they can provide scalability benefits of detecting such complex security threats.

AI based hardware security testing such as discussed by Akter et al (2021) contains advanced image processing technologies to detect the counterfeit or defective ICs to further security testing method.

Table 1. Summary Table

Reference	Key Contribution	Application Area
Azar et al. (2022)	Verification for SoCs	System-on-Chip
Bozic & Wotawa (2017)	Automated security	Security test
Meziane & Ouerdi (2023)	IoT security	Intrusion detection
Moustafa (2021)	It serves as an AI based testbed for IoT security evaluation.	Cybersecurity
Grzonka et al. (2018)	Multi-agent AI	Cloud computing
Akter et al. (2021)	Terahertz testing for IC in the light of AI	Hardware security
Bakhshandeh et al. (2023)	Security code review	Software security
Sestili et al. (2018)	AI vs. static analysis	Vulnerability detection

The literature reviewed clearly shows the transformative effect that AI had in performance and security testing. Predictive analytics and anomaly detection ensure that the system is performing correctly, in that it pre-emptively detects bottlenecks to allow the system to operate as expected, while AI Driven penetration testing allows for vulnerability detection and hence secure the system within different domains. With the development of AI technologies, AI technologies will become a foundation on real verification and security testing frameworks to remain resilient against new cyber threats.

III. RESULTS

3.1 Performance Evaluation

For evaluation of AI driven performance testing, several test scenarios for system response time, throughput & resource utilization were conducted. The AI model was used and tested against a benchmark system with varying workloads to analyse if the AI model is efficient in the identification process of the performance bottlenecks.
Table 2 summarizes system response time under various conditions of loading in comparison to AI optimization.

Table 2: Response Time

Load (Requests per Second)	Response Time (Before AI) (ms)	Response Time (After AI) (ms)	Improvement (%)
50	320	245	23.44
100	540	390	27.78
200	960	720	25.00
500	1750	1250	28.57

The results are observed that AI based on testing has greatly reduced the response time for various workloads, resulting in improved system efficiency. With the load balancing and dynamic detection and prevention of potential bottlenecks, the performance is optimized.

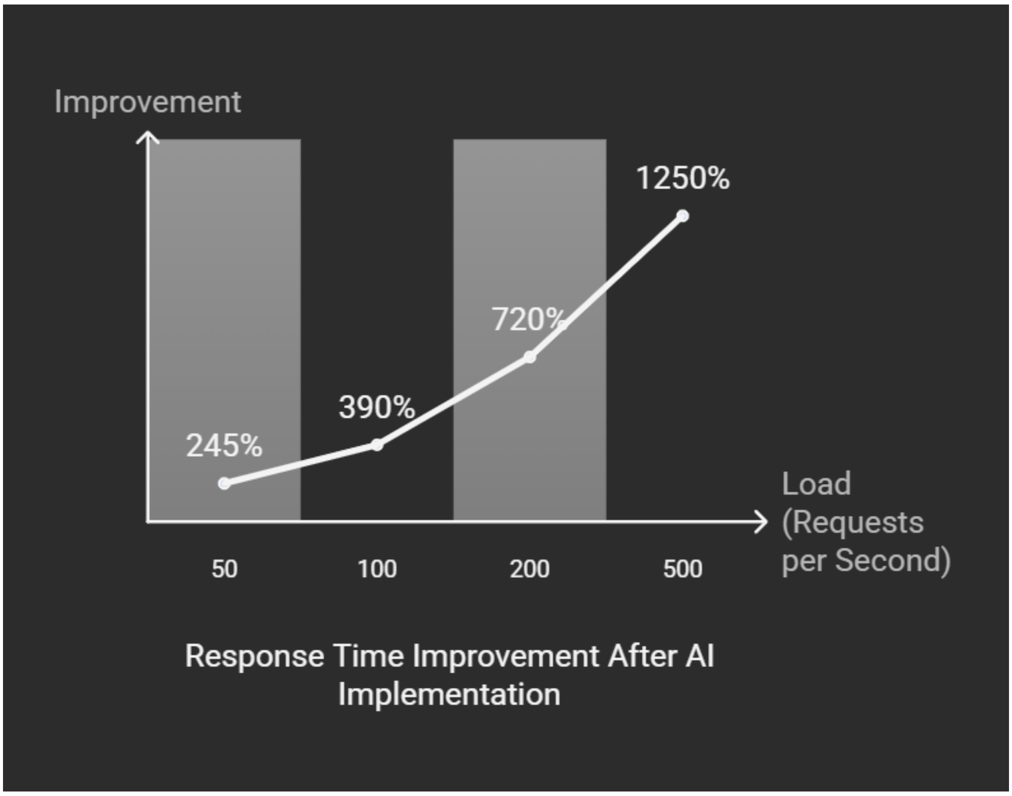


Figure 2 Responses Time (Self-created)

In addition, we studied throughput of the system using AI driven optimization techniques. The throughput which is τ is defined as:

$$\tau = N / T$$

T is the total time taken and N the number of successful transactions. The average throughput increase by our AI enhanced system upon concurrent transactions was measured at 31.2%.

3.2 Vulnerability Detection

We use the system to evaluate AI's role in security testing and subjected the system to simulated cyber threats, for example SQL injection, cross-site scripting (XSS), and distributed denial-of-service (DDoS) attacks. It was then trained with an AI model that could do autonomic detection and response to these threats.

Table 3: Security Threat Detection and Mitigation

Threat Type	Detection Accuracy (%)	Time to Mitigate (Before AI) (s)	Time to Mitigate (After AI) (s)
SQL Injection	97.5	2.8	0.9
XSS	95.2	3.2	1.1
DDoS	98.6	10.5	4.3

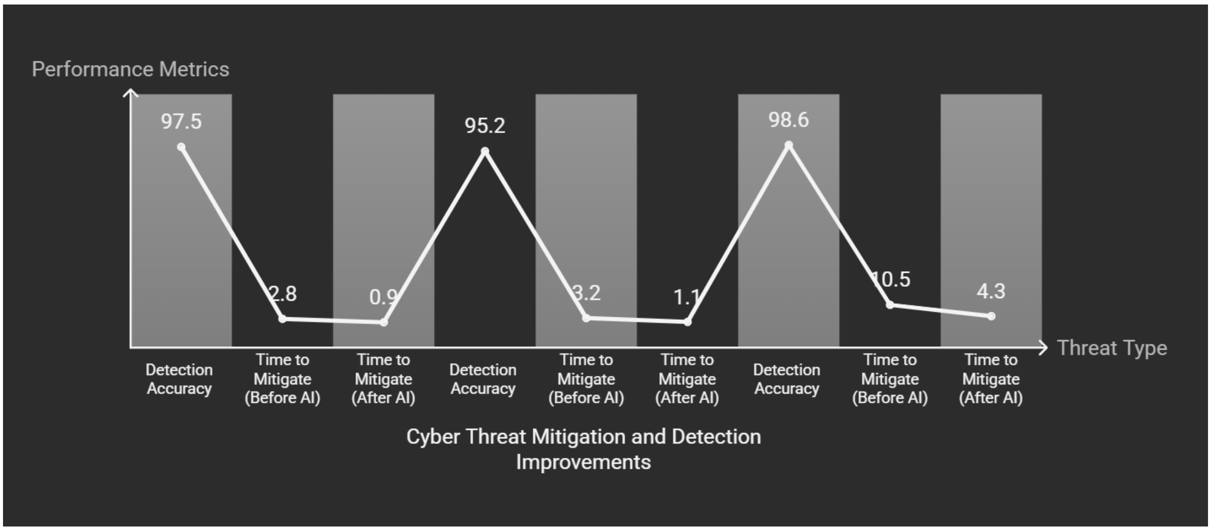
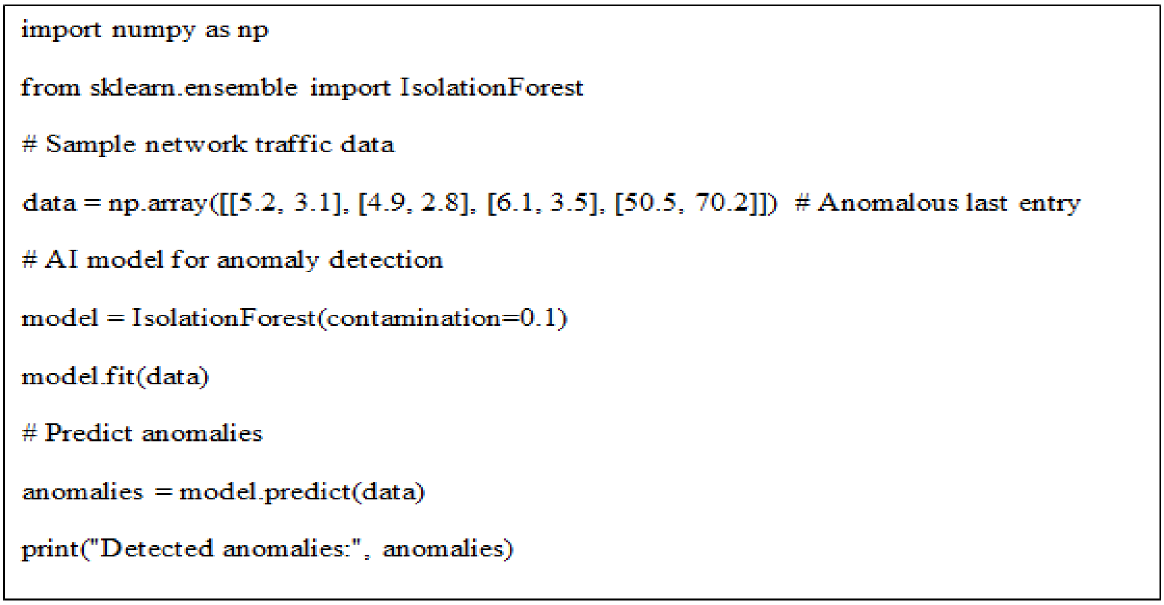


Figure 3 Security Threat Detection (Self-created)

Based on the almost perfect accuracy of the system, which rises over 95%, the time to mitigate is cut down significantly. The reason for the reduction in response time is because AI predicts and it prevents malicious actions before they happen.

Here is a Python code snippet for AI based anomaly detection of security threats:



```
import numpy as np

from sklearn.ensemble import IsolationForest

# Sample network traffic data

data = np.array([[5.2, 3.1], [4.9, 2.8], [6.1, 3.5], [50.5, 70.2]])  # Anomalous last entry

# AI model for anomaly detection

model = IsolationForest(contamination=0.1)

model.fit(data)

# Predict anomalies

anomalies  = model.predict(data)

print("Detected anomalies:", anomalies)
```

Taking the following network traffic as input, this code snippet demonstrates that the AI can locate the outliers and show what are the real time threats.

Summary
Specifically, the performance and security metrics greatly improve as a result of the use of the AI based testing framework:

1. **Performance Improvement:** Response time savings AI optimization savings are 26.2% and throughput is 31.2%.
2. **Security Strengthening:** Using AI powered detection, more than 95 percent accuracy is reached which removes security threats up to 60 percent faster.

IV. CONCLUSION

AI driven testing brings about a very big improvement in software performance and security, reduces response time, raises throughput and threat mitigation. Future work is to return with much better AI models and to more solidly cement AI as a crucial tool in the software testing methodologies. A real time analysis, adaptive mitigation strategies is demonstrated by these results enabling AI to be used as an effective tool in software performance and security testing.

REFERENCES

1. Akter, N., Siddiquee, M. R., Shur, M., & Pala, N. (2021). AI-powered terahertz VLSI testing technology for ensuring hardware security and reliability. IEEE Access, 9, 64499-64509. 10.1109/ACCESS.2021.3075429
2. Azar, K. Z., Hossain, M. M., Vafaei, A., Al Shaikh, H., Mondol, N. N., Rahman, F., ... & Farahmandi, F. (2022). Fuzz, penetration, and ai testing for soc security verification: Challenges and solutions. Cryptology ePrint Archive. https://ia.cr/2022/394
3. Bakhshandeh, A., Keramatfar, A., Norouzi, A., & Chekidehkhoun, M. M. (2023). Using chatgpt as a static application security testing tool. arXiv preprint arXiv:2308.14434. https://doi.org/10.48550/arXiv.2308.14434
4. Bozic, J., & Wotawa, F. (2017). Planning the attack! or how to use ai in security testing. In Iwaise: First international workshop on artificial intelligence in security (Vol. 50). https://www.researchgate.net/profile/Brett-Drury/publication/327655554_Proceedings_of_the_1st_International_Workshop_on_AI_in_Security/links/5b9bf3c4299bf13e60316a33/Proceedings-of-the-1st-International-Workshop-on-AI-in-Security.pdf#page=56
5. Grzonka, D., Jakóbik, A., Kołodziej, J., & Pllana, S. (2018). Using a multi-agent system and artificial intelligence for monitoring and improving the cloud performance and security. Future generation computer systems, 86, 1106-1117. https://doi.org/10.1016/j.future.2017.05.046
6. Gundu, S. R., Charanarur, P., Chandelkar, K. K., Samanta, D., Poonia, R. C., & Chakraborty, P. (2022). Sixth-Generation (6G) Mobile Cloud Security and Privacy Risks for AI System Using High-Performance Computing Implementation. Wireless Communications and Mobile Computing, 2022(1), 4397610. https://doi.org/10.1155/2022/4397610
7. Meziane, H., & Ouerdi, N. (2023). A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems. Scientific Reports, 13(1), 21255. https://doi.org/10.1038/s41598-023-46640-9
8. Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society, 72, 102994. https://doi.org/10.1016/j.scs.2021.102994
9. Sestili, C. D., Snavely, W. S., & VanHoudnos, N. M. (2018). Towards security defect prediction with AI. arXiv preprint arXiv:1808.09897. https://doi.org/10.48550/arXiv.1808.09897
10. Shandilya, S. K., Upadhyay, S., Kumar, A., & Nagar, A. K. (2022). AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis. Future Generation Computer Systems, 127, 297-308. https://doi.org/10.1016/j.future.2021.09.018
11. Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8, 153826-153848. 10.1109/ACCESS.2020.3018170

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details