International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 10 | Oct - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Towards Intelligent Cyber Defence: Leveraging Artificial Immune Systems and General Intelligence

Dr. U. Sivaji[(a)] Ganta Varshala[(1)], Rayudu Yamini Sameera[(2)], Jakkula Uday Kiran[(3)]
(1-3) Department of Information Technology, (a)guide of project,
Institute of Aeronautical Engineering, Hyderabad, Telangana, India
varshalaganta@gmail.com, yaminirayudu@gmail.com, udaykiranyadav123456@gmail.com

Abstract: This paper addresses how the integration of Artificial General Intelligence (AGI) and Artificial Immune Systems (AIS) may enhance the Security Operations Centers (SOCs) performance. We use a hypothetical case study, mathematical models, and calculate the number of true positives, false positives, detection accuracy between AGI-driven AIS and traditional AI based AIS to compare both working methods in relation to major parameters. Overall results indicate that AIS driven by AGIs has the potential to increase the threat detection, optimize the operational efficiency, and minimize investments. This evidence indicates that the implementation of AGI into SOCs may revolutionize cybersecurity by offering resource-optimization, rationalization of processes, and enhanced resistance to the evermore advanced types of threats. The current study shows the significance of AGI to governments, manufacturers, cybersecurity experts, and investors who are in need of more efficient security systems.

Keywords: Artificial General Intelligence (AGI), Artificial Immune Systems (AIS), Security Operations Centers (SOCs), Cybersecurity, Threat Detection, Operational Efficiency, AI-driven Security, Resource Optimization, False Positives, True Positives.

I. INTRODUCTION

Cybersecurity is moving into a new phase in which the level of sophistication and complexity of the threat requires sophisticated defense systems that will be dynamic. Combining Artificial General Intelligence (AGI) and Artificial Immune Systems (AIS) is an exciting direction of the threats detection and response. Security Operations Centers (SOCs) have the potential to gain greater effect in detecting malicious activity, more efficient response times, and climbing success rates in fighting cyberspace threats with the potential convergence of both factors; the capability of AGI to generalise across tasks and the bio-inspired flexibility of AIS.

Recent research has discussed the synergy of such applications of AGI with AIS whereby the integration can perform better than conventional AI-based AIS system in various key SOC performance measures that include; true positive, benign negative, false positive, and false negative [1]. The developments are strategic to organizations and government agencies wishing to minimize incidents of cybersecurity activities within a complex digital environment.

The AIS has been demonstrated in the Internet of Things (IoT) field to be promising as a highly adaptive, self-learning defensive mechanism where the Internet of Things devices have limited resources and are subject to compromise. Experimental evidence also shows that artificial immune model variations, like the Negative Selection Algorithm (NSA), and the Artificial Immune Network (AIN), provide good scalability and cyber defense at scale in IoT networks [2]. This flexibility means that AIS could be feasible security solution in fast developing and dynamic infrastructures.

Cybersecurity is also being transformed by Large Language Models (LLMs) such as through abilities in in-context learning, instruction following, and step-by step reasoning. When improved with timely engineering, these abilities allow LLMs to perform complicated tasks, such as cryptographic tasks, without being explicitly programmed. Through such models, the paradigm around AI in cybersecurity will be able to support more than specific algorithms because encryption, decryption, and secure key use can be learned instead of hard-coded [3].

Artificial Intelligence (AI) in general has emerged as a sensitive instrument against the modern cyber attacks. The literature encompasses the use of AI in threat prevention, reaction, and realization and the ethical issues surrounding it and the inefficiencies to be expected. It is advised that a mutual effort should be taken up by policymakers, organizations, and security experts, to make AI as useful as possible [4]. Co-promoting AGI achievements has occurred in the form of multimodal foundation models to process visual and textual data to achieve cross-modal learning and transfer. Fei et al. show that these models can be generalized to various tasks without being task-specific trained, and are one step closer to AGI-like behaviors [5].

Nevertheless, the dangers of AGI do evoke fears of losing control, misaligned motives, and social disruption and should engage proactive safety infrastructures and governance [6]. Our proposed framework provides a new cybersecurity system in which the AGI is integrated with AIS to create an intelligent, adaptive, and scalable defense system proposed in this paper. Combining the reasoning and learning capabilities of AGI and the dynamic threat detection of AIS we are able to improve

SOC operations, lessen false alerts, and allocate resources optimally. We use hypothetical case studies and mathematical modeling to show that through AGI-driven AIS, it is possible to design more robust and efficient cybersecurity than through the conventional approach, offering a new paradigm of cybersecurity.

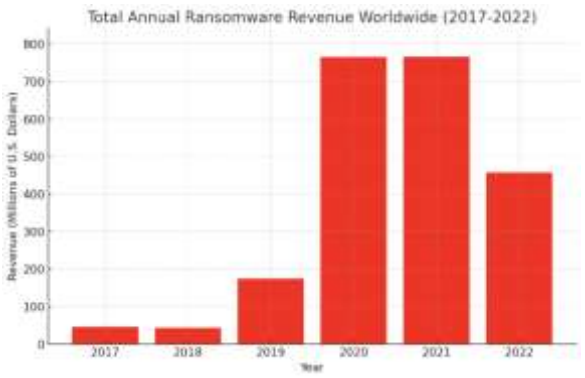

Figure 1: Money received by ransomware

II. LITERATURE SURVEY

This paper is a review of how Artificial General Intelligence (AGI) could be combined with Artificial Immune Systems (AIS) to boost Security Operations Centers (SOCs). AC using a hypothetical case-study and mathematical modeling compares AGI driven AI enforced AIS with conventional AI-based AIS on major SOC measures which include true positives, benign positives, false positives, and false negatives. Findings indicate integrated AGI leads to higher accuracy of detecting and higher operational efficiency as well as cost-effectiveness, which can be of great benefit compared to conventional AI methodologies. This approach reinforces the threat detection system, simplifies the work of the SOC, and makes the most of available resources to potential consumers, which includes the government agencies, OEMs, cybersecurity specialists, and investors [1].

The IoT has led to the growth of connectivity and automation, with the associated security violations because weak device safeguards are present. The traditional security systems tend to be ineffective in such dynamic environments. Taking a cue out of the human immune system, AIS offers adaptive self-learning protection that can support fast responses to threats in real-time. An overview of six models of AIS to Internet of Things security reveals that Negative Selection Algorithm (NSA) and Artificial Immune Network (AIN) perform better and scale highly to indicate the ability of AIS to secure large and dynamic IoT networks [2].

The sharp increase in the use of the technology of the large language models (LLMs) is transforming cyber security because the complex features of this technology, such as in-context learning, instruction following, and step-by-step reasoning, allow them to address other issues and solve complex problems with no need to go through the training process. Prompt engineering further optimises their performance, and in cryptography, LLMs can also have an end-to-end adversarial learning strategy, where they can handle encryption, decryption, and confidentiality goals directly out of training objectives. This represents LLMs as an important step to artificial general intelligence (AGI) and also shows knowledge gaps and technological issues [3].

The use of AI is becoming more prevalent to deal with the constantly mounting complexity of worldwide cybersecurity risks, aiding in threat detection, prevention, and response in the occurrence of an incident. Nevertheless, AI-based security systems are not without problems as ethical issues and technical shortcomings are also present. According to literature and case studies, integrating approaches carefully, perpetual advancement, and cooperation among policymakers, organizations as well as security specialists seems necessary to enhance digital fortification and resilience against an evolving cyber-related threat [4].

To step in the direction of AGI, Fei et al. (2022) introduce a multimodal foundation model trained with laxly related image text pairs via large-scale self-supervised learning. and inspired by the idea that the human brain represents modality invariant concepts, it performs transfer learning and cross-modal comprehension, and an imagined capacity to produce conceptually related results other than straightforward recognition. In spite of its potential on the variety of cognitive tasks that no task-specific training is required, it suffers due to needing rigorous benchmarking to confirm its AGI-like abilities [5].

McLean et al. (2023) provide a systematic review to investigate the risks that can be associated with Artificial General Intelligence (AGI) by referring to the body of scholarly literature, policy reports, and expert suggestions. The paper subdivides the risks into the technical, ethical and societal domains, raising the concerns of the loss of human control, unintended or inappropriate goals, vulnerability to security attacks, and major socio-economic disruption. It points out the fact that the risk generated by AGI due to its ability to work autonomously across multiple fields in increased significantly in the event of its emergence even more so when it is unclear what directions it will take and how it will be managed. The authors present the need to implement proactive risk assessment, strong safety systems, and interdisciplinary cooperation to evaluate the highly multifaceted challenge of AGI and point out that early mitigation measures are essential to provide positive and manageable deployments of AGI. [6]

III. PROPOSED METHOD

In this study, the author presents a technology to assess the inclusion of Artificial General Intelligence (AGI) with Artificial Immune Systems (AIS) in order to improve Security Operations Centers (SOCs). The methodology integrates a theoretical model, mathematical presentation, and the hypothetical case study in a sequential comparison of AGI-powered AIS with the conventional AI-driven AIS by attributing the feasibility of threat detection performance and operational efficiency.

1. System Modeling: The SOC environment is emulated in terms of important performance indicators, such as true positives, false positives, false negatives and benign positives. AIS driven by AGI is oriented to resemble adaptive and self-learning characteristics following the human immune system, whereas the pre-disposed detection rules are presented in traditional AI-driven AIS.
2. Hypothetical Case Study: The hypothetical SOC is modeled using realistic network traffic, synthetic cyber-attacks, and non-attacks. This enables comparisons between AGI driven AIS and AI driven AIS on a controlled basis under the same operating conditions.
3. Mathematical Formulation: Mathematical formulations are used to measure performance in terms of mathematical equations and statistical models. Cost-Benefit Analysis (CBA) will be utilized in estimating a possible monetary advantage and the Technology Acceptance Model (TAM) will be utilized to assess financial advantage and acceptance of the fabricated.
4. Step-by-Step Evaluation: This is the portion of the methodology that employs stepwise calculations of the detection accuracy, operational efficiency and resource optimization. False positive and false negative are discussed in to bring out the sources of mistakes and possible corrections.
5. Validation and Analysis: There will be a comparison of the result of AGI-driven AIS and AI-driven AIS in order to validate the results based on the improvement of detection rates, response time, and cost-effectiveness. Weaknesses that include the lack of biological skills in the AIS designing are mentioned in order to inform future interdisciplinary study.

These methodologies also focuses on transparency, replicability, and practical relevancy, illustrating how AGI can revolutionize the SOC business and improve the detection of threats, as well as allocate resources in more strategic ways, which provides a strategic benefit to both governments, cybersecurity experts, and companies operating the industries.

IV. RESULT

Enhancing cyber threat detection in IoT systems requires advanced approaches beyond traditional machine learning and deep learning techniques. Models such as ANN, CNN, RNN, and LSTM have been applied for identifying attacks, but their reliance on individual logic reduces overall accuracy. To address this limitation, a stacked hybrid framework (ACLR) was designed by integrating ANN, CNN, LSTM, and RNN. This combination leverages the unique advantages of each algorithm, resulting in more effective detection of cyber-attacks across IoT networks.

The ACLR model was tested on the UNSW15 dataset**,** which includes 15 categories of attacks. Training was carried out with a batch size of 32, 30 epochs, and a KFOLD value of 1 to

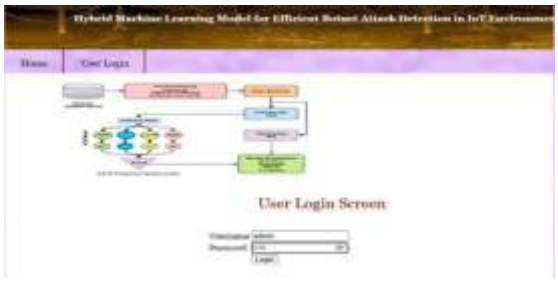

Figure 2: User Login

balance efficiency and computational cost. Evaluation metrics included Accuracy, Precision, Recall, F-Score, Confusion Matrix, and ROC analysis. Models such as ANN, CNN, RNN, and LSTM have been applied for identifying attacks, but their reliance on individual logic reduces overall accuracy. Findings revealed that the hybrid ACLR approach consistently outperformed individual models, offering superior accuracy and detection capability, thereby making it a more dependable method for IoT cybersecurity.

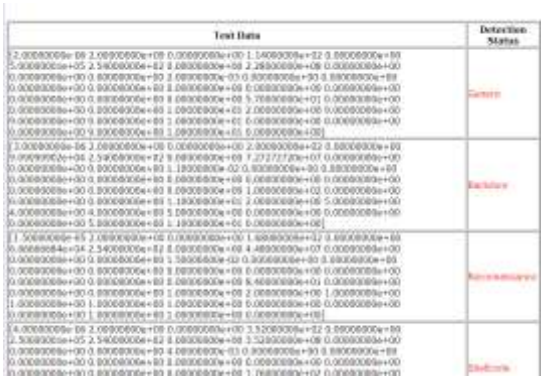

Figure 3: Test Data.csv

CONCLUSION

This study investigates the potential of AGI-driven Artificial Immune Systems (AIS) to enhance the efficiency of Security Operations Centers (SOCs) by comparing them with traditional AI-driven AIS using mathematical models.

Through a hypothetical case study grounded in realistic data and supported by frameworks like Cost-Benefit Analysis (CBA) and the Technology Acceptance Model (TAM), the research analyzes key SOC metrics, revealing improvements in true positives and reductions in false positives and false negatives. The transparent, step-by-step methodology ensures reliability and replicability, while also highlighting potential operational efficiencies and financial savings. Although limited by the absence of biological expertise, the study provides a strong foundation for future interdisciplinary research, demonstrating that AGI-driven AIS can transform cybersecurity defenses, optimize resource allocation, and improve incident response within SOCs.

V. REFERENCES

1. Falowo, Olufunsho I., Lily Botsyoe, Kehinde Koshoedo, and Murat Ozer. "Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response." IEEE Access (2024).
2. Sharma, Prianka, and Kaylash Chaudhary. "Adaptive Cybersecurity for IoT Networks Using Artificial Immune Systems: A Scalable Approach for Real-Time Threat Detection." In International Conference on Artificial Intelligence on Textile and Apparel, pp. 733-746. Singapore: Springer Nature Singapore, 2024.
3. Pleshakova, Ekaterina, Aleksey Osipov, Sergey Gataullin, Timur Gataullin, and Athanasios Vasilakos. "Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends." Journal of Computer Virology and Hacking Techniques 20, no. 3 (2024): 429-440.
4. Jimmy, Fnu. "Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses." Valley International Journal Digital Library 1 (2021): 564-74.
5. N. Fei, Z. Lu, Y. Gao, G. Yang, Y. Huo, J. Wen, H. Lu, R. Song, X. Gao, T. Xiang, H. Sun, and J.-R. Wen, "Towards artificial general intelligence via a multimodal foundation model," Nature Commun., vol. 13, no. 1, p. 3094, Jun. 2022.
6. S. McLean, G. J. M. Read, J. Thompson, C. Baber, N. A. Stanton, and P. M. Salmon, "The risks associated with artificial general intelligence: A systematic review," J. Experim. Theor. Artif. Intell., vol. 35, no. 5, pp. 649–663, Jul. 2023.
7. D. Dasgupta, "An overview of artificial immune systems and their applications," in Artificial Immune Systems and Their Applications, 20, pp. 3–21.
8. U. Aickelin, D. Dasgupta, and F. Gu, "Artificial immune systems," in Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques. Cham, Switzerland : Springer, 2013, pp. 187–211.
9. J. Timmis, T. Knight, L. N. de Castro, and E. Hart, "An overview of artificial immune systems," in Computation in Cells and Tissues: Perspectives and Tools of Thought, 2004, pp. 51–91.
10. D. Dasgupta, "Immuno-inspired autonomic system for cyber defense," Inf. Secur. Tech. Rep., vol. 12, no. 4, pp. 235–241, 2020.