IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 12 August 2024, accepted 2 September 2024, date of publication 4 September 2024,
date of current version 12 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3454543

RESEARCH ARTICLE

Enhancing Cybersecurity With Artificial Immune Systems and General Intelligence: A New Frontier in Threat Detection and Response

OLUFUNSHO I. FALOWO[1], LILY EDINAM BOTSYOE[1], KEHINDE KOSHOEDO[2], AND MURAT OZER[1]

[1]School of Information Technology, University of Cincinnati, Cincinnati, OH 45221, USA
[2]School of Built Environment, Faculty of Technology, Environment and Design, Oxford Brookes University, OX3 0BP Oxford, U.K.

Corresponding author: Olufunsho I. Falowo (falowooi@mail.uc.edu)

ABSTRACT This study explores how integrating Artificial General Intelligence (AGI) with Artificial Immune Systems (AIS) could potentialy enhance the efficiency of Security Operations Centers (SOCs). By employing a hypothetical case study and mathematical models, this research compares AGI-driven AIS with traditional AI-driven AIS across key SOC metrics such as True Positives, Benign Positives, False Positives, and False Negatives. Our analysis reveals that AGI-driven AIS solution offers notable improvements in detection accuracy and operational efficiency while reducing costs. These findings highlight the transformative potential of AGI in bolstering cybersecurity defenses. This research emphasizes the importance of AGI for SOCs, presenting it as a critical advancement over current AI technologies. This is particularly relevant for government regulators, original equipment manufacturers (OEMs), cybersecurity professionals, and investors. This study attempts to provide a compelling evidence that AGI can drive more effective and efficient SOC operations, encouraging stakeholders to consider investing in and adopting these advanced AI technologies. In a landscape where cybersecurity threats are becoming increasingly sophisticated, the integration of AGI with AIS to build security threat detection and response, represents a promising frontier. This research underscores the potential of AGI to not only enhance detection and response capabilities but to also streamline operations and optimize resource allocation within SOCs. The findings in this study, we argue, suggest that AGI could play a pivotal role in the future of cybersecurity, making it an essential consideration for those looking to stay ahead in the ongoing battle against cyber threats.

INDEX TERMS Artificial general intelligence (AGI), artificial immune system (AIS), cybersecurity, security operations center (SOC), threat detection, incident response, true positives, false positives, cost savings, operational efficiency, government regulation.

I. INTRODUCTION

The concept of Artificial Immune System (AIS) draws inspiration from the discipline of Biological Sciences, especially from biological immune system discourse, which not only has evolved over many decades of years but have shaped understanding of the detection and neutralization of harmful pathogens [1], [2]. AIS according to Timmis et al. [3] is defined as ''computational systems inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving''. Although ''the first international conference on artificial immune systems (ICARIS) took place at the University of Kent at Canterbury (UKC) in September 2002'' [3] but it was initially conceptualized in decades prior that conference, and has since matured into a robust computational paradigm designed to emulate the adaptive and dynamic responses of its biological counterpart. In biology, the immune system's capability to recognize and remember organism that caused disease to its host, while adapting to new threats has been important

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

area of study. This same principle has over recent decades been applied to the field of cybersecurity, where AIS models continuously learn and evolve to detect, identify, and mitigate threats in an ever-changing digital landscape.

The intersection of AIS with cybersecurity incident detection and response has shown significant promise [4], [5], [6], [7]. AIS-based systems are designed to identify anomalies and recognize patterns indicative of malicious activities, much like how biological immune systems detect foreign invaders [4], [5], [6], [7]. By mimicking the immune system's mechanisms of learning and memory, AIS-driven cybersecurity technology tend to mature over time to adapt to new threats and improve over time, providing a dynamic defense mechanism that evolves with the threat landscape [4], [5], [6], [7]. This adaptability is crucial for proactive and real-time threat detection, which is essential for effective incident response in modern cybersecurity environments.

Despite the advancements, there remain gaps and untapped potential in the integration of Artificial General Intelligence (AGI) [8], [9], [10], [11], [12], [13], [14], [15] with AIS for cybersecurity applications. AGI, still in the the early stages of theoretical development, with its ability to understand, learn, and apply knowledge across a wide range of tasks [8], [9], [10], [11], [12], [13], [14], [15], could significantly enhance the capabilities of AIS. Integrating AGI with AIS could lead to more sophisticated and autonomous systems capable of anticipating and mitigating complex cyber threats before they even materialize. Exploring this integration could uncover new methodologies for efficient detection and defense, transforming the cybersecurity landscape. The potential for AGI-enhanced AIS to provide a holistic and anticipatory approach to threat management underscores the necessity for continued research and development in this field, aiming to create more resilient and adaptive cybersecurity infrastructures.

With reference to Figure 1 and Figure 2, historical data from 2017 to 2022 reveals a significant and alarming upward trend in ransom payments made to threat actors, underscoring the escalating threat posed by cybercriminal activities [16]. As organizations increasingly rely on digital infrastructures, the sophistication of cyberattacks has evolved, resulting in more devastating consequences and higher ransom demands. The financial burden placed on organizations by these ransomware attacks, coupled with the critical need to restore operations swiftly, has driven companies to pay increasingly exorbitant sums. This trend highlights the inadequacy of existing cybersecurity measures and the urgent need for more effective and adaptive solutions to mitigate these threats.

Based on Figure 2, a forecast was calculated and plotted in Figure 3. This forecasts leveraged the ETS forecasting model [17], [18] and outcome of that calculation suggest that this upward trend in ransom payments will continue as cybercriminals become more adept at exploiting vulnerabilities within digital ecosystems. This anticipated rise further underscores the critical importance of continued research into innovative cybersecurity strategies, such as the integration of Artificial Immune Systems (AIS) and Artificial General Intelligence (AGI). By enhancing the ability to detect and respond to sophisticated cyber threats in real-time, these advanced technologies promise to improve the overall efficiency of cybersecurity operations, reducing the financial and operational impacts of cyberattacks. In this context, the exploration of AIS and AGI offers a proactive approach to fortifying digital defenses, aiming to reverse the troubling trend of increasing ransomware payments.

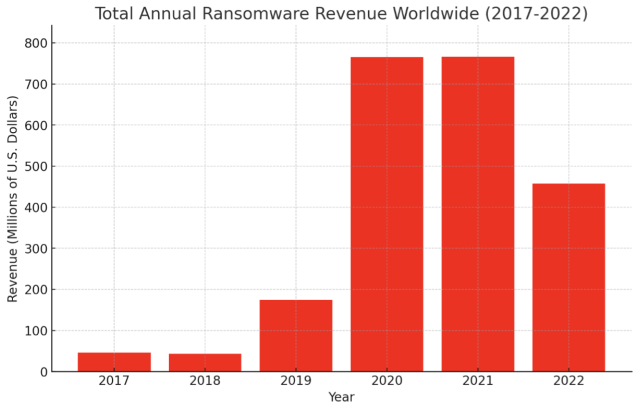

FIGURE 1. Money received by ransomware actors [19].

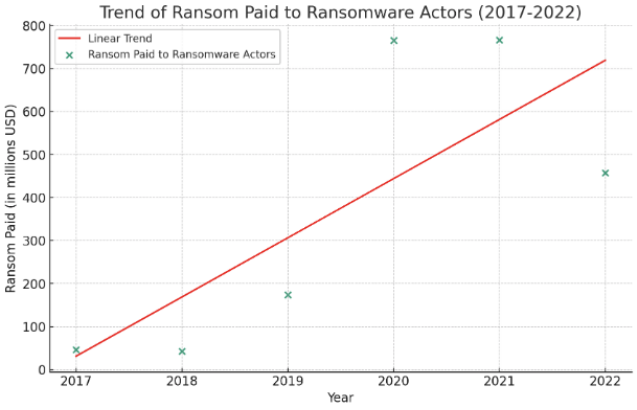

FIGURE 2. Trend of money received by ransomware actors.

II. REVIEW OF EXISTING LITERATURE

A. JUXTAPOSITION: NATURAL IMMUNITY VS ARTIFICIAL IMMUNITY VS ARTIFICIAL IMMUNITY SYSTEM

Natural immunity refers to the body's biological defense system that identifies and combats pathogens like bacteria and viruses [20], [21], [22]. It relies on a complex network of cells and molecules to recognize and remember invaders, providing long-term protection [20], [21], [22]. Artificial immunity involves medical interventions, such as vaccines, that stimulate the immune system to develop resistance to specific pathogens without causing the disease [20], [21], [22]. AIS, on the other hand, are computational models inspired by natural immunity, designed to detect and respond to anomalies and threats in cybersecurity, adapting and

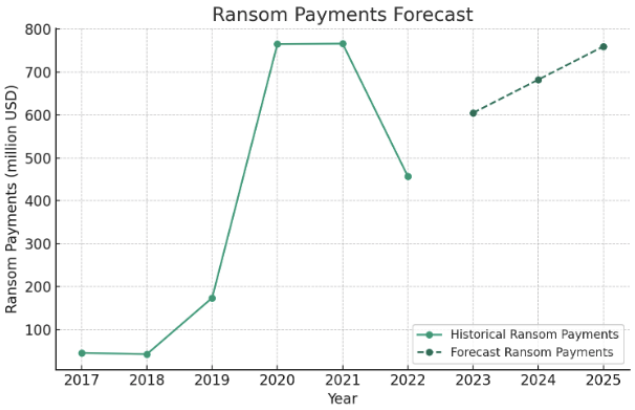

FIGURE 3. ETS ransom payment forecast.

learning to protect digital environments just as biological systems protect living organisms [1], [2].

B. EVOLUTION OF AIS MODELS

Dipankar Dasgupta, an IEEE Fellow, NAI Fellow, and IEEE Distinguished Lecturer, is a Hill Professor of Computer Science at The University of Memphis. His research encompasses computational intelligence, cybersecurity, immunological computation, and generative AI. Dasgupta has conducted numerous well-cited studies on artificial immune systems, significantly contributing to the field and advancing the understanding and application of bio-inspired methods in cybersecurity and beyond. The synthesis of studies by Dipankar Dasgupta and other researchers highlights the evolution of several key models and principles within AIS. One fundamental model is the Clonal Selection Algorithm (CSA), which is described to have features that could mimic the biological process of clonal selection where immune cells proliferate and differentiate in response to pathogens [23], [24], [25], [26], [27], [28]. This model is argued to be instrumental in optimization problems and pattern recognition. Another important principle is the Negative Selection Algorithm (NSA), inspired by the immune system's ability to distinguish between self and non-self cells, crucial for anomaly detection and cybersecurity applications [23], [24], [25], [26], [27], [28]. The Artificial Immune Network (AIN) model extends this by representing a network of interacting antibodies that can adapt and learn over time, providing robust solutions for data clustering and adaptive control systems [23], [24], [25], [26], [27], [28].

Additionally, the Danger Theory, proposed by Polly Matzinger, shifts the focus from self/non-self recognition to the detection of danger signals, offering a new perspective on immune response and leading to novel approaches in AIS for intrusion detection [23], [24], [25], [26], [27], [28]. The Immune Network Theory, which describes the regulation of the immune system through networks of antibodies, has also been adapted into computational models that excel in pattern recognition and data visualization [23], [24], [25], [26], [27], [28]. Furthermore, principles of Affinity Maturation and Hypermutation, which describe the immune system's process of improving antibody affinity through iterative mutations, have been incorporated into AIS to enhance learning algorithms and optimization techniques [23], [24], [25], [26], [27], [28]. These models and principles collectively illustrate the dynamic and adaptive nature of AIS, making them powerful tools in computational intelligence and cybersecurity.

1) SELF AND NON-SELF DISTINCTION

The idea of self and non-self is central to many AIS models, reflecting the biological immune system's critical function of distinguishing between the body's own cells and foreign invaders [29], [30], [31]. This concept is fundamental in models such as the NSA, which is designed to detect anomalies by generating detectors that recognize non-self elements, thus identifying potential threats in cybersecurity. The self/non-self paradigm is also significant in the CSA, where immune cells are selected based on their ability to recognize non-self antigens, thereby optimizing responses to unfamiliar challenges. By emulating this biological distinction, AIS models can effectively identify and respond to cyber threats, enhancing the adaptability and robustness of cybersecurity defenses. The evolution of this idea in AIS has led to more sophisticated and reliable methods for detecting and mitigating security breaches.

2) DANGER THEORY

Danger Theory, proposed by Polly Matzinger, revolutionizes the traditional self/non-self recognition paradigm by emphasizing the detection of danger signals emitted by stressed or damaged cells, rather than merely identifying foreign entities [32], [33], [34], [35]. This theory posits that the immune system responds to signals indicating cellular distress or damage, which can be caused by both internal and external factors, rather than strictly differentiating between self and non-self. In the context of Artificial Immune Systems (AIS), Danger Theory provides a novel approach to intrusion detection by focusing on abnormal behavior and environmental context rather than predefined patterns of malicious activity. This shift enables AIS to more effectively enable the identification and response to emerging threats by recognizing the underlying signs of potential danger, thereby enhancing the system's ability to adapt to new and unforeseen cyber threats.

3) EXPLAINER: MATHEMATICAL LOGIC OF AIS MODELS

- Clonal Selection Algorithm (CSA), as described by Castro and Zuben [36], mathematically models the biological clonal selection process to optimize and learn from a population of solutions. The algorithm begins by evaluating the affinity of each antibody (solution) to an antigen (problem). Antibodies with higher affinity are selected and cloned in proportion to their affinity [36]. These clones then undergo mutation

at a rate inversely proportional to their affinity, ensuring that better solutions mutate less [36]. The mutated clones are re-evaluated, and the best-performing antibodies are selected to form a new population [36]. This iterative process continues until a termination criterion is met, enabling the algorithm to converge on optimal or near-optimal solutions [36]. This CSA framework effectively balances exploration and exploitation in the solution space, leveraging principles of biological immunity for computational problem-solving.

- The Negative Selection Algorithm (NSA), as described by Castro and Timmis [37], begins by defining a set of self-patterns representing normal system states. A large number of candidate detectors are then randomly generated. Each detector is evaluated against the self-patterns, and those that do not match any self-pattern are retained [37]. These validated detectors are deployed to monitor new data, identifying anomalies when new patterns match any of the detectors. The algorithm relies on an affinity measure to quantify similarity and a threshold to define allowable matches, ensuring that only non-self patterns trigger an anomaly detection. This process mimics the immune system's ability to recognize and respond to foreign entities, providing a robust mechanism for identifying deviations from normal behavior [37].
- The Artificial Immune Network (AIN), models a dynamic network of interacting antibodies to solve computational problems [37]. Each antibody represents a potential solution, and their similarity is quantified using an affinity measure. Antibodies are connected if their affinity exceeds a threshold [37]. High-affinity antibodies are cloned and mutated, with mutation rates inversely proportional to their affinity to maintain solution quality. A suppression mechanism eliminates highly similar antibodies to preserve diversity. The network evolves by continuously updating with new antibodies and removing less effective ones, ensuring adaptability and robustness in problem-solving. This model captures the immune system's dynamic interactions and learning capabilities for computational applications [37].
- The Danger Theory, shifts from traditional self/non-self models to focus on detecting danger signals emitted by stressed or damaged cells [32], [33], [34], [35], [38]. In AIS, this is mathematically represented by categorizing signals into safe (S_{safe}) and danger (S_{danger}) signals. For each pattern p, a signal $s(p)$ is assigned as either safe or dangerous. Antigens (a) are associated with these signals, and an affinity function affinity(a, s) quantifies the relationship, triggering an immune response if this affinity exceeds a threshold θ. The threshold θ is dynamically updated based on the history of signals, ensuring the system adapts to new threats. This formulation emphasizes the detection of actual harm rather than the mere presence of foreign entities, leading to more context-aware and accurate threat detection in cybersecurity systems [32], [33], [34], [35], [38].

C. IMPACT OF BIG DATA ON THE EVOLUTION OF ARTIFICIAL IMMUNE SYSTEMS

The advent of big data has significantly contributed to the evolution of AIS by providing vast amounts of diverse and complex data that AIS can analyze and learn from [39], [40], and [41]. Big data enables AIS to improve its anomaly detection and response mechanisms by identifying patterns and correlations in large datasets that were previously unmanageable. This enhanced learning capability allows AIS to adapt more effectively to emerging threats, optimize its algorithms, and develop more sophisticated models for cybersecurity, ultimately leading to more robust and dynamic defense systems.

D. BIO-INSPIRED CYBERSECURITY DEFENSES

Drawing on these immunological principles, AIS has emerged as a powerful tool in computational intelligence, particularly in the field of cybersecurity. By mimicking the biological capabilities of the immune system's mechanisms, as described in prior paragraphs, AIS can detect anomalies and recognize patterns indicative of malicious activities. This bio-inspired approach has led to the development of sophisticated algorithms capable of identifying zero-day attacks and sophisticated malware that traditional methods might miss [42], [43]. AIS's dynamic learning and adaptive capabilities enable it to respond to new and evolving threats in real-time, providing a proactive defense mechanism. The integration of these immunological concepts into computational models has significantly enhanced the effectiveness of cybersecurity incident detection and response, offering a resilient and evolving solution to protecting digital infrastructure.

1) RANSOMWARE: DARK WEB ECONOMY

The evolution of AIS has significantly enhanced cybersecurity defenses against ransomware [42], [43], [44], a prevalent threat in the Dark Web economy. AIS models, such as the Clonal Selection Algorithm and the Negative Selection Algorithm as described in prior paragraphs are designed to mimic the adaptive and memory capabilities of the biological immune system. These models continuously monitor and learn from network activities to detect and respond to anomalies indicative of ransomware or other malware attacks. By using immune network theory, AIS can dynamically recognize and neutralize ransomware signatures and behaviors, even those that are previously unknown. The integration of danger theory allows AIS to detect stress signals from systems under attack, providing early warning and rapid response to minimize damage. This adaptive, real-time detection and response mechanism makes AIS a powerful tool in protecting against the evolving and sophisticated tactics employed by ransomware distributed through the Dark Web.

2) HOW AIS AND AI SYNERGY ENHANCES THREAT DETECTION AND RESPONSE IN SOCs

AIS have directly influenced how artificial intelligence (AI) enhances threat detection and response in Security Operations Centers (SOC) by providing adaptive learning and anomaly detection mechanisms inspired by the human immune system [45], [46]. AIS models, such as the Clonal Selection Algorithm and Negative Selection Algorithm, as described in prior paragraphs, utilize AI to continuously learn from network behavior and historical attack data. This allows the system to identify true positives by recognizing genuine threats with high accuracy. The adaptive nature of AIS enables AI to update detection rules dynamically, reducing false positives caused by outdated or incorrect alert logic.

Moreover, AIS enhances the identification of benign positives by using AI to analyze contextual information, distinguishing between legitimate but unusual activities and actual threats. This reduces unnecessary alerts and allows SOC analysts to focus on real incidents. By leveraging AI's advanced data processing capabilities, AIS improves the accuracy of data inputs, minimizing false positives from inaccurate data. Additionally, the combination of AIS and AI enhances the detection of false negatives by identifying complex and evolving threat patterns that traditional methods might miss, ensuring a comprehensive and effective security operation in SOCs.

E. EXPLORING THE POTENTIAL OF AGI-DRIVEN AIS FOR ENHANCED SOC EFFICIENCY

Although AGI remains a theoretical construct and is in its early stages of development, its potential to surpass traditional AI systems makes it a compelling focus for research, particularly at the intersection with AIS. AGI is envisioned to possess a broader understanding and adaptability, capable of learning and reasoning across diverse tasks without human intervention. When integrated with AIS, which already leverages biologically inspired models for adaptive threat detection and response, AGI could significantly enhance the precision and efficiency of security operations. By analyzing complex patterns and evolving threats in real-time, AGI-driven AIS could improve True Positive and Benign Positive rates, while further reducing False Positives and False Negatives, thereby optimizing SOC performance.

The significance of researching the intersection of AIS and AGI lies in the potential to revolutionize how SOCs operate. Current AIS models have proven effective in improving cybersecurity metrics, but the integration of AGI could bring a transformative leap. AGI's ability to understand context, learn from minimal data, and adapt to novel threats could enhance the adaptability and resilience of AIS, leading to more accurate threat detection and fewer erroneous alerts. This study aims to mathematically demonstrate these potential improvements, providing a robust framework for evaluating the efficiency gains in SOCs. By exploring this intersection, this study can pave the way for more advanced and autonomous cybersecurity systems, ultimately leading to a safer digital environment.

F. RESEARCH QUESTION

AIS have significantly improved the efficiency of SOC by leveraging biologically inspired mechanisms to enhance threat detection and response. Existing literature demonstrates that AIS models, such as the Clonal Selection Algorithm and Negative Selection Algorithm, contribute to our understanding of the improvement of key metrics including True Positives, Benign Positives, and reduce False Positives and False Negatives. With the advent of AGI, there is potential for even greater advancements to be unravelled. The research question highlighted in bullet point below, aims to mathematically compare AGI-driven AIS with AI-driven AIS to determine if AGI can further enhance SOC efficiency by improving detection accuracy and reducing erroneous alerts.

- How can mathematical models be utilized to demonstrate that AGI-driven AIS enhances the efficiency of Security Operations Centers (SOCs) compared to AI-driven AIS solutions, with respect to improving True Positives, Benign Positives, reducing False Positives (due to incorrect alert logic and inaccurate data), and minimizing False Negatives?

III. METHODOLOGY

A. VALIDATING AGI-DRIVEN AIS: THEORETICAL AND MATHEMATICAL ASSUMPTIONS

As this study explores the potential of AGI-driven AIS in enhancing SOC efficiency, it is crucial to understand the fundamental mathematical and theoretical assumptions underlying this study. First, AIS as deduced from existing literature, operates on the principle of adaptive learning and anomaly detection, inspired by the human immune system's ability to recognize and respond to diverse pathogens. This involves continuously updating and refining detection algorithms based on new data, which improves the identification of true positives and reduces false positives and negatives. The assumption here is that the dynamic and self-learning nature of AIS can be significantly enhanced by AGI's broader and more flexible learning capabilities, which can handle more complex and varied threat patterns with minimal human intervention.

Also, the theoretical assumption is that AGI, with its advanced cognitive abilities, will outperform traditional AI by better understanding context and making more accurate predictions. This means AGI-driven AIS can dynamically adapt to novel and evolving cyber threats more effectively than AI-driven systems. Mathematically, this study attempts to posit that AGI's ability to process and analyze vast datasets with higher accuracy will lead to superior SOC metrics–higher true positives, better management of benign positives, and reduced false positives and false negatives. By validating these assumptions through mathematical

models, this paper aim to demonstrate that the integration of AGI with AIS represents a transformative advancement in the future of cybersecurity, offering unparalleled efficiency and robustness in threat detection and response.

B. HYPOTHETICAL CASE STUDY

Using a hypothetical case study as part of the methodology for this study provides a controlled environment to rigorously analyze the potential benefits of AGI-driven AIS over AI-driven AIS. This approach allows us to systematically apply mathematical models to simulate real-world scenarios, ensuring the results are not influenced by external variables that could skew the data. It enables us to isolate and evaluate the specific impacts of AGI-driven improvements on key metrics, such as True Positives, False Positives, and overall cost efficiency in Security Operations Centers (SOCs), thereby providing a clear and measurable justification for the proposed advancements. Below is the hypothetical case study:

In this hypothetical SOC managed by Cybersecurity Experts Inc., the organization handles approximately 150 cybersecurity incidents annually- where they operate in a 24 by 7 three shift model. According to a publication titled "Cost of Cyber Incidents: Systematic Review & Cross-Validation" published by Cybersecurity & Infrastructure Security Agency (CISA) in 2020, the weighted average investigation cost per incident is $66,935.3 [47]. This hypothetical SOC currently utilizes an AI-driven AIS to manage and respond to these incidents. However, the system encounters challenges with high false positive rates and occasional false negatives, leading to increased investigation times and costs.

With the theoretical implementation of an AGI-driven AIS, this study hypothesize an improvement in detection accuracy, resulting in a 25% reduction in the number of incidents requiring in-depth investigation due to better identification and classification of threats. Additionally, a 15% improvement in the efficiency of handling true positives and benign positives is expected, reducing unnecessary alert fatigue and optimizing resource allocation.

- **Note:** The name "Cybersecurity Experts Inc" referenced in the case study is purely hypothetical and is not intended to refer to any existing entity.

IV. RESULTS: PER MATHEMATICAL MODELS FOR SOC METRICS

By showing these calculations, breaking down these formulas step-by-step and explaining their components, as shown in this section, this study attempt to make it accessible for individuals without a mathematical background to grasp how each metric is calculated and its importance in evaluating SOC performance. Detailed explanations of the mathematical models are crucial for understanding the reliability and validity of the metrics, ensuring clarity in how AGI-driven AIS enhancements could significantly improve security operations. This approach underscores the practical implications and benefits, encouraging informed decision-making in cybersecurity. This study systematically calculate each metric for both AI-driven AIS and AGI-driven AIS. The step-by-step calculations are crucial for transparency and replicability of the study. Below, are the performance differences in SOC metrics and estimate annual cost savings where applicable.

A. TRUE POSITIVE (TP)

Explanation: True Positives measures the number of correctly identified threats. It is crucial for understanding the effectiveness of the detection system in identifying real incidents.

Formula:

$$TP = \sum_{i=1}^{N} \mathbb{1}(\text{actual}_i = 1 \wedge \text{predicted}_i = 1) \tag{1}$$

Components:

- $\sum_{i=1}^{N}$: Summation over all incidents.
- $\mathbb{1}$(condition): Indicator function, equals 1 if the condition is true, 0 otherwise.
- actual_i: Actual state of the i-th incident (1 if a real threat, 0 if not).
- predicted_i: Predicted state of the i-th incident by the system (1 if identified as a threat, 0 if not).

Mathematical Assumptions: The models assume accurate labeling of actual states and correct implementation of prediction algorithms.

AI-driven AIS SOC: Assuming the current system correctly identifies 60% of the 150 incidents:

$$TP_{\text{AI}} = 150 \times 0.60 = 90 \tag{2}$$

AGI-driven AIS SOC: Assuming AGI-driven AIS improves TP by 15%, the new TP can be calculated as:

$$TP_{\text{AGI}} = TP_{\text{AI}} \times 1.15 = 90 \times 1.15 = 103.5 \tag{3}$$

B. BENIGN POSITIVE (BP)

Explanation: Benign Positives measures the number of legitimate activities that are flagged as threats but are actually non-malicious. It is important for understanding the system's ability to distinguish between threats and non-threats.

Formula:

$$BP = \sum_{i=1}^{N} \mathbb{1}(\text{actual}_i = 0 \wedge \text{predicted}_i = 1 \wedge \text{contextual}_i = 1) \tag{4}$$

Components:

- $\sum_{i=1}^{N}$: Summation over all incidents.
- $\mathbb{1}$(condition): Indicator function, equals 1 if the condition is true, 0 otherwise.
- actual_i: Actual state of the i-th incident (0 if not a real threat).
- predicted_i: Predicted state of the i-th incident by the system (1 if identified as a threat).

- contextual$_i$: Contextual information indicating the incident is expected to be non-malicious (1 if true).

Mathematical Assumptions: The models assume correct contextual labeling and accurate predictions.

AI-driven AIS SOC: Assuming the current system flags 20 benign positives out of 150 incidents:

$$BP_{\text{AI}} = 20 \tag{5}$$

AGI-driven AIS SOC: Assuming AGI-driven AIS improves BP by 15%, the new BP can be calculated as:

$$BP_{\text{AGI}} = BP_{\text{AI}} \times 1.15 = 20 \times 1.15 = 23 \tag{6}$$

C. FALSE POSITIVE (FP) - INCORRECT ALERT LOGIC

Explanation: False Positives due to incorrect alert logic measure non-threats flagged as threats due to detection logic flaws.

Formula:

$$FP_{IAL} = \sum_{i=1}^{N} \mathbb{1}(\text{actual}_i = 0 \wedge \text{predicted}_i = 1) - BP \tag{7}$$

Components:

- $\sum_{i=1}^{N}$: Summation over all incidents.
- $\mathbb{1}$(condition): Indicator function, equals 1 if the condition is true, 0 otherwise.
- actual$_i$: Actual state of the i-th incident (0 if not a real threat).
- predicted$_i$: Predicted state of the i-th incident by the system (1 if identified as a threat).
- BP: Benign Positives.

Mathematical Assumptions: Assumes that the BP calculation is accurate and the alert logic has known flaws.

AI-driven AIS SOC: Assuming the current system incorrectly flags 30 incidents as threats due to incorrect alert logic:

$$FP_{IAL_{\text{AI}}} = 30 - BP_{\text{AI}} = 30 - 20 = 10 \tag{8}$$

AGI-driven AIS SOC: Assuming AGI-driven AIS reduces FP by 20%, the new FP can be calculated as:

$$FP_{IAL_{\text{AGI}}} = FP_{IAL_{\text{AI}}} \times 0.80 = 10 \times 0.80 = 8 \tag{9}$$

D. FALSE POSITIVE (FP) - INACCURATE DATA

Explanation: False Positives due to inaccurate data measure non-threats flagged as threats due to bad data inputs.

Formula:

$$FP_{ID} = \sum_{i=1}^{N} \mathbb{1}(\text{actual}_i = 0 \wedge \text{predicted}_i = 1 \wedge \text{data}_i = 0) \tag{10}$$

Components:

- $\sum_{i=1}^{N}$: Summation over all incidents.
- $\mathbb{1}$(condition): Indicator function, equals 1 if the condition is true, 0 otherwise.
- actual$_i$: Actual state of the i-th incident (0 if not a real threat).
- predicted$_i$: Predicted state of the i-th incident by the system (1 if identified as a threat).
- data$_i$: Data accuracy indicator (0 if inaccurate).

Mathematical Assumptions: Assumes accurate assessment of data accuracy.

AI-driven AIS SOC: Assuming the current system flags 10 incidents as threats due to inaccurate data:

$$FP_{ID_{\text{AI}}} = 10 \tag{11}$$

AGI-driven AIS SOC: Assuming AGI-driven AIS reduces FP by 20%, the new FP can be calculated as:

$$FP_{ID_{\text{AGI}}} = FP_{ID_{\text{AI}}} \times 0.80 = 10 \times 0.80 = 8 \tag{12}$$

E. FALSE NEGATIVE (FN)

Explanation: False Negatives measures the number of actual threats that are incorrectly identified as non-threats. It is crucial for understanding the risk of missed detections.

Formula:

$$FN = \sum_{i=1}^{N} \mathbb{1}(\text{actual}_i = 1 \wedge \text{predicted}_i = 0) \tag{13}$$

Components:

- $\sum_{i=1}^{N}$: Summation over all incidents.
- $\mathbb{1}$(condition): Indicator function, equals 1 if the condition is true, 0 otherwise.
- actual$_i$: Actual state of the i-th incident (1 if a real threat).
- predicted$_i$: Predicted state of the i-th incident by the system (0 if not identified as a threat).

Mathematical Assumptions: Assumes accurate labeling of actual states and correct implementation of prediction algorithms.

AI-driven AIS SOC: Assuming the current system misses 20% of actual threats:

$$FN_{\text{AI}} = 150 \times 0.20 = 30 \tag{14}$$

AGI-driven AIS SOC: Assuming AGI-driven AIS reduces FN by 25%, the new FN can be calculated as:

$$FN_{\text{AGI}} = FN_{\text{AI}} \times 0.75 = 30 \times 0.75 = 22.5 \tag{15}$$

F. ANNUAL COST SAVINGS

Explanation: Annual cost savings are calculated based on the reduction in the number of incidents requiring in-depth investigation.

Formula:

$$\text{Cost Savings} = (N_{\text{AI}} - N_{\text{AGI}}) \times \$66,935.3 \tag{16}$$

Components:

- N_{AI}: Number of incidents investigated under AI-driven AIS.
- N_{AGI}: Number of incidents investigated under AGI-driven AIS.
- \$66,935.3: Average cost per incident investigation.

Assuming a 25% reduction in the number of incidents:

$$N_{\text{AGI}} = N_{\text{AI}} \times 0.75 = 150 \times 0.75 = 112.5 \quad (17)$$

Therefore, the cost savings can be calculated as:

$$\text{Cost Savings} = (150 - 112.5) \times \$66,935.3 \quad (18)$$

$$\text{Cost Savings} = 37.5 \times \$66,935.3 = \$2,510,073.75 \quad (19)$$

This analysis above demonstrates the potential financial and operational benefits of implementing AGI-driven AIS in SOCs. Table 1 provides a tabular presentation of all the results, clearly illustrating the performance metrics of AI-driven AIS compared to AGI-driven AIS. This table highlights the significant improvements achieved with AGI-driven AIS, including increased True Positives and Benign Positives, and reduced False Positives and False Negatives. By systematically displaying these gains, the table effectively demonstrates the superior efficiency and cost savings potential of AGI-driven AIS in enhancing Security Operations Centers (SOCs).

TABLE 1. Comparison of AI-driven AIS and AGI-driven AIS Metrics.

Metric	AI-driven	AGI-driven
True Positive (TP)	90	103.5
Benign Positive (BP)	20	23
False Positive (FP) - Incorrect Alert Logic	10	8
False Positive (FP) - Inaccurate Data	10	8
False Negative (FN)	30	22.5

V. DISCUSSION

A. THEORETICAL FRAMEWORKS SUPPORTING THE METHODOLOGY

Relying on the Cost-Benefit Analysis (CBA) and Technology Acceptance Model (TAM) frameworks provides a robust basis for the methodology used in this study, by combining economic and user-centered perspectives. Through the lens of CBA, this paper ensure evaluation of the financial benefits of AGI-driven AIS, highlighting cost savings and resource optimization, which are critical for justifying investments in new technology. TAM, on the other hand, emphasizes the importance of perceived usefulness and ease of use, ensuring that the improvements in detection accuracy and operational efficiency are likely to be accepted and integrated by SOC professionals, leading to smoother implementation and greater overall effectiveness.

1) COST-BENEFIT ANALYSIS (CBA)

CBA is a theoretical framework that assesses the economic value of investments and decisions by comparing the costs and benefits [48], [49], [50], [51]. This CBA theory highlights the importance of quantifying the financial savings of AGI-driven AIS over AI-driven AIS. By calculating the cost reduction from improved incident handling efficiency, this framework provides a clear economic justification for adopting AGI-driven AIS. With reliance on CBA as a guide, this paper argue, will help decision-makers understand the tangible financial benefits, reinforcing the superiority of AGI-driven AIS in reducing investigation costs and optimizing resource allocation.

2) TECHNOLOGY ACCEPTANCE MODEL (TAM)

The TAM explains how users come to accept and use a technology based on perceived usefulness and ease of use [52], [53], [54], [55]. This framework provides the ground for this study by highlighting the improvements in SOC efficiency and accuracy with AGI-driven AIS, which are likely to increase user acceptance and adoption. By demonstrating enhanced True Positives and reduced False Positives and Negatives through mathematical models, this study show that AGI-driven AIS not only performs better but is also more reliable and efficient, making it more acceptable to SOC professionals. This acceptance leads to smoother integration and greater overall effectiveness in cybersecurity operations.

B. SIGNIFICANT FINANCIAL BENEFITS OF AGI-DRIVEN AIS FOR GLOBAL SOCs

The final cost savings calculated from implementing AGI-driven AIS in the SOC amounts to approximately $2,492,078.75 annually. This significant reduction in investigation costs highlights the potential financial benefits for organizations with global SOCs, where resource optimization and cost-efficiency are paramount. By improving detection accuracy and reducing the number of incidents requiring in-depth investigation, AGI-driven AIS not only enhances operational efficiency but also frees up valuable resources for proactive cybersecurity measures, strategic initiatives, and overall better management of global cybersecurity threats.

C. ENSURING RELIABILITY AND VALIDITY

This study satisfies the theory of reliability [56], [57] by providing a detailed, replicable methodology for comparing AI-driven and AGI-driven AIS in Security Operations Centers (SOCs). By using standardized metrics such as True Positives, False Positives, and False Negatives, and employing well-established mathematical models, the research ensures that the results are consistent and can be replicated by other researchers under similar conditions. The step-by-step calculations and clear presentation of data enhance the reliability of the findings, making it easier for others to verify and validate the results independently.

In terms of validity [56], [57], the study ensures both internal and external validity by carefully designing the hypothetical case study and using realistic data points, such as the average cost of investigating a cybersecurity incident. The theoretical frameworks of CBA and TAM, this study also argue, support the validity of this study by providing a comprehensive evaluation of both the financial and user acceptance aspects of AGI-driven AIS. This dual focus ensures that the findings are not only statistically sound but also practically relevant, offering significant insights

into the potential benefits and challenges of implementing AGI-driven AIS in global SOCs.

D. THE PRACTICAL IMPLICATIONS OF INTEGRATING AGI AND AIS

The results of this study underscore the importance of integrating AGI with AIS to enhance Security vis-a-vis SOC efficiency. By demonstrating significant improvements in key metrics such as True Positives and reductions in False Positives and Negatives, the study highlights how AGI-driven AIS can optimize threat detection and response processes. This integration not only enhances operational efficiency but also leads to substantial cost savings, as shown by the estimated annual reduction in investigation costs.

Moreover, conducting research that marries AGI and AIS provides a practical framework for evaluating SOC performance in real-world scenarios. The use of mathematical models and hypothetical case studies ensures that the findings are both reliable and valid, offering a clear and measurable justification for the proposed advancements. This balanced approach ensures that the benefits of AGI-driven AIS are not only theoretically sound but also practically applicable, making a compelling case for organizations to consider adopting this advanced technology to enhance their cybersecurity posture.

E. ADVANCING CYBERSECURITY: INTEGRATING AGI AND AIS FOR INCIDENT DETECTION AND RESPONSE

This study holds significant importance for cybersecurity incident detection and response by illustrating the transformative potential of integrating AGI with AIS. For leadership and industry cybersecurity leaders, the findings demonstrate that AGI-driven AIS can substantially enhance SOC efficiency by improving key metrics such as True Positives and reducing False Positives and False Negatives. This improvement not only ensures more accurate threat detection but also optimizes resource allocation, leading to a more robust and proactive cybersecurity posture.

For Original Equipment Manufacturers (OEMs) and cybersecurity solution providers, this study is intended to provides a clear and measurable justification for investing in AGI-driven AIS technologies. The demonstrated cost savings and operational efficiencies highlight the practical benefits of adopting advanced AI solutions to meet the evolving threat landscape. By leveraging AGI's superior learning capabilities, OEMs can potentially develop more effective cybersecurity tools that enhance incident response capabilities, ultimately offering better protection for their clients and strengthening their market position in the cybersecurity industry.

F. STUDY LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

One limitation of this study is the reliance on a hypothetical case study and mathematical models, which may not fully capture the complexities and nuances of real-world SOC environments. The controlled environment used for analysis might oversimplify the variability and unpredictability inherent in actual cybersecurity incidents. This study attempted to balance this by using realistic data points, such as the average investigation cost, and by grounding this research's methodology in established theoretical frameworks like Cost-Benefit Analysis (CBA) and the Technology Acceptance Model (TAM). However, the extrapolation of these findings to diverse organizational contexts should be done cautiously.

Future interdisciplinary studies should explore the integration of AGI and AIS in more varied and complex SOC settings, incorporating real-world data and scenarios. Collaborations between cybersecurity experts, AI researchers, and industry practitioners can provide a more comprehensive understanding of the practical implications and challenges of implementing AGI-driven AIS. Additionally, longitudinal studies assessing the long-term impacts of AGI integration on SOC efficiency and effectiveness would be valuable. Such research could further validate the potential benefits and address any unforeseen limitations, ensuring that the transition to AGI-driven AIS is both feasible and beneficial for organizations worldwide.

G. ENCOURAGING AGI RESEARCH FOR FUTURE MARKET READINESS

Although AGI is still in its early stages and largely a theoretical construct, OEMs are actively racing to bring AGI to market in the future due to its transformative potential. Encouraging research in this area is crucial, as it lays the groundwork for practical applications and addresses challenges early on. By fostering interdisciplinary studies and exploring AGI's integration with technologies like Artificial Immune Systems (AIS), researchers can drive innovation, improve cybersecurity defenses, and ensure that future implementations are both effective and secure.

H. PRIVACY CONCERNS ARISING FROM THE COMMERCIALIZATION OF AGI IN SOC ACTIVITIES

Government regulators play a crucial role in the future of AGI-driven AIS, ensuring that ethical standards [58], [59] are maintained while fostering innovation. As these advanced systems become integral to cybersecurity, regulators must establish guidelines that address privacy, data protection, and transparency. This includes setting standards for how AGI-driven AIS can be deployed, monitored, and audited to prevent misuse or unintended consequences. By balancing the need for robust cybersecurity with ethical considerations, regulators can help build public trust and ensure that the deployment of AGI-driven AIS aligns with societal values and legal frameworks.

The commercialization of Artificial General Intelligence (AGI) introduces substantial privacy concerns [11], particularly when AGI is implemented in Security Operations Centers (SOCs) that manage large volumes of sensitive data. AGI systems, equipped with advanced analytical capabilities,

are likely to gain access to extensive datasets, including personal and confidential information. This elevated level of access significantly heightens the risk of data breaches, unauthorized access, and the misuse of personal data. For instance, during the monitoring and analysis of network traffic, AGI systems could unintentionally expose or mishandle sensitive information, leading to severe privacy violations. Moreover, the ability of AGI to process and correlate data from multiple sources could result in the unnecessary collection and retention of personal data, further intensifying privacy risks [60].

The importance of addressing these privacy concerns through ethical frameworks has been emphasized in existing research, such as the work by Kelly et al. (2020). Initially perceived as a market differentiator, the ethical framework for AGI systems now serves a pivotal role in mitigating privacy risks. Companies that prioritize ethical practices and protocols for AGI systems can leverage their commitment to build consumer trust and navigate complex regulatory requirements more effectively. Additionally, making AGI protocols publicly available promotes transparency and encourages collective innovation, driving the adoption of privacy-preserving technologies. This open approach accelerates the development of ethically aligned AGI systems and ensures that privacy considerations are integral to their design from the outset. Therefore, addressing consumer privacy concerns is crucial for the successful commercialization of AGI systems [61].

I. ADDRESSING POTENTIAL BIAS

This study, conducted by cybersecurity experts, might exhibit potential biases due to the absence of immunologists and biological scientists. The focus on existing literature from AIS and AGI researchers may have limited the depth of interdisciplinary insights that are crucial for a comprehensive understanding of the biological underpinnings of AIS. This could lead to an overemphasis on technological aspects while underestimating the complexities and nuances of biological principles that drive immune system-inspired models.

However, the study attempts to balance these potential biases by thoroughly referencing well-established works from experts in AIS and AGI. By grounding the research in robust theoretical frameworks such as Cost-Benefit Analysis (CBA) and the Technology Acceptance Model (TAM), the study ensures a rigorous methodological approach. Additionally, the hypothetical case study and reliance on realistic data points provide a practical perspective, which helps in mitigating some of the limitations arising from the lack of direct biological expertise. Future research should incorporate interdisciplinary collaborations to enhance the robustness and validity of findings.

J. BROADER CONTRIBUTIONS TO ACADEMIC KNOWLEDGE: CONNECTING AGI, AIS, AND SOC METRICS

This study attempts to connect Artificial General Intelligence (AGI), Artificial Immune Systems (AIS), and Security Operations Center (SOC) metrics to show potential possibilities of enhancements in cybersecurity operations. This study echoes the promises of AGI and discusses how AGI-driven AIS solutions could leverage advanced intelligence to improve threat detection and response metrics, such as True Positives and False Positives, within SOCs. By demonstrating significant improvements in these metrics, this study highlights the potential of AGI-driven AIS solutions to optimize SOC efficiency and reduce operational costs. The broader contribution to academic knowledge lies in providing a robust, quantifiable framework for evaluating the integration of AGI in cybersecurity, encouraging further interdisciplinary research and practical applications in enhancing global cybersecurity defenses.

K. THOUGHT-PROVOKING PREDICTION ROOTED IN AGI AND AIS INTEGRATION

Given the maturity of AIS in enhancing computational capabilities and the human-like cognitive and decision-making potential of AGI, this study predicts a transformative leap in cybersecurity. Within the next decade, AGI-driven AIS systems (or tools) will not only surpass current AI systems' capabilities in SOCs but will also evolve to autonomously manage and mitigate complex cyber threats with minimal human intervention. This advanced system will adapt in real-time, learning from each incident to preemptively counteract emerging threats, fundamentally changing the landscape of cybersecurity defense.

This bold prediction suggests that AGI-driven AIS will become an indispensable tool for global cybersecurity incident response, capable of anticipating and neutralizing attacks before they can inflict damage. This proactive approach will significantly reduce the cost and impact of cyber incidents, enabling organizations to allocate resources more effectively. This paradigm shift will stimulate further interdisciplinary research, driving innovations that merge cognitive science, machine learning, and cybersecurity to create systems that not only react but also foresee and strategize against potential cyber threats, ensuring a safer digital future.

VI. CONCLUSION

This study systematically addresses the research question by employing mathematical formulas to compare AGI-driven AIS with AI-driven AIS in enhancing the efficiency of Security Operations Centers (SOCs). By using a hypothetical case study grounded in realistic data points and established theoretical frameworks like Cost-Benefit Analysis (CBA) and the Technology Acceptance Model (TAM), the study provides a comprehensive analysis of key SOC metrics. The results demonstrate significant improvements in True Positives and reductions in False Positives (due to incorrect alert logic and inaccurate data) and False Negatives, validating the hypothesis that AGI-driven AIS offers superior performance.

Moreover, the detailed step-by-step calculations and transparent methodology ensure the reliability and replicability of

the findings, offering a clear and measurable justification for the proposed advancements. The study highlights not only the operational efficiencies but also the substantial financial savings that arguably may be achieved by implementing AGI-driven AIS systems. While acknowledging the limitations due to the absence of biological expertise, the research sets a strong foundation for future interdisciplinary studies to further explore and validate the potential of AGI-driven AIS in real-world SOC environments. This comprehensive approach underscores the transformative potential of AGI in advancing cybersecurity defenses and elevating how we conduct cybersecurity incident response.

REFERENCES

[1] D. Dasgupta, "An overview of artificial immune systems and their applications," in *Artificial Immune Systems and Their Applications*, 1999, pp. 3–21.

[2] 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.

[3] 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.

[4] D. Dasgupta, "Immuno-inspired autonomic system for cyber defense," *Inf. Secur. Tech. Rep.*, vol. 12, no. 4, pp. 235–241, 2007.

[5] D. Dasgupta, "Advances in artificial immune systems," *IEEE Comput. Intell. Mag.*, vol. 1, no. 4, pp. 40–49, Nov. 2006.

[6] J. Zhao, S. Guo, and D. Mu, "Model design of artificial immune system in power cyber security protection," in *Proc. 2nd Int. Conf. Appl. Mach. Learn. (ICAML)*, Oct. 2020, pp. 7–11.

[7] P. Wlodarczak, "Cyber immunity: A bio-inspired cyber defense system," in *Proc. Int. Conf. Bioinf. Biomed. Eng.*, Granada, Spain. Cham, Switzerland: Springer, 2017, pp. 199–208.

[8] 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.

[9] B. Goertzel, "Artificial general intelligence: Concept, state of the art, and future prospects," *J. Artif. Gen. Intell.*, vol. 5, no. 1, pp. 1–48, Dec. 2014.

[10] B. Goertzel, *Artificial General Intelligence*, vol. 2. New York, NY, USA: Springer, 2007.

[11] S. Baum, "A survey of artificial general intelligence projects for ethics, risk, and policy," Global Catastrophic Risk Inst., Washington, DC, USA, Working Paper 17-1, 2017.

[12] 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.

[13] F. Dou et al., "Towards artificial general intelligence (AGI) in the Internet of Things (IoT): Opportunities and challenges," 2023, *arXiv:2309.07438*.

[14] O. I. Obaid, "From machine learning to artificial general intelligence: A roadmap and implications," *Mesopotamian J. Big Data*, pp. 81–91, Aug. 2023.

[15] K. W. Carlson, "Safe artificial general intelligence via distributed ledger technology," *Big Data Cognit. Comput.*, vol. 3, no. 3, p. 40, Jul. 2019.

[16] O. I. Falowo, S. Popoola, J. Riep, V. A. Adewopo, and J. Koch, "Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents," *IEEE Access*, vol. 10, pp. 134038–134051, 2022.

[17] O. I. Falowo, M. Ozer, C. Li, and J. B. Abdo, "Evolving malware and DDoS attacks: Decadal longitudinal study," *IEEE Access*, vol. 12, pp. 39221–39237, 2024.

[18] O. I. Falowo and J. B. Abdo, "2019–2023 in review: Projecting DDoS threats with ARIMA and ETS forecasting techniques," *IEEE Access*, vol. 12, pp. 26759–26772, 2024.

[19] Statista. (2024). *Annual Amount of Money Received by Ransomware Actors Worldwide From 2017 to 2022*. Accessed: Jan. 25, 2024. [Online]. Available: https://www.statista.com/statistics/1410498/ransomware-revenue-annual/

[20] K. M. Ariful Kabir and J. Tanimoto, "Analysis of individual strategies for artificial and natural immunity with imperfectness and durability of protection," *J. Theor. Biol.*, vol. 509, Jan. 2021, Art. no. 110531.

[21] E. Klarreich, "Inspired by immunity," *Nature*, vol. 415, no. 6871, pp. 468–470, Jan. 2002.

[22] O. Loew, "On natural and artificial immunity," *Science*, vol. 20, no. 516, pp. 356–357, Dec. 1892.

[23] F. A. González and D. Dasgupta, "Anomaly detection using real-valued negative selection," *Genetic Program. Evolvable Mach.*, vol. 4, pp. 383–403, Jan. 2003.

[24] D. Dasgupta and F. Gonzalez, "An immunity-based technique to characterize intrusions in computer networks," *IEEE Trans. Evol. Comput.*, vol. 6, no. 3, pp. 281–291, Jun. 2002.

[25] D. Dasgupta and N. Attoh-Okine, "Immunity-based systems: A survey," in *Proc. IEEE Int. Conf. Syst., Man, Cybern., Comput. Cybern. Simulation*, vol. 1, 1997, pp. 369–374.

[26] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2011, pp. 1–8.

[27] F. Hosseinpour, K. A. Bakar, A. H. Hardoroudi, and N. Kazazi, "Survey on artificial immune system as a bio-inspired technique for anomaly based intrusion detection systems," in *Proc. Int. Conf. Intell. Netw. Collaborative Syst.*, Nov. 2010, pp. 323–324.

[28] D. Zegzhda, E. Pavlenko, and E. Aleksandrova, "Modelling artificial immunization processes to counter cyberthreats," *Symmetry*, vol. 13, no. 12, p. 2453, Dec. 2021.

[29] S. T. Wierzchoń, "Deriving a concise description of non-self patterns in an artificial immune system," in *New Learning Paradigms in Soft Computing*, 2002, pp. 439–464.

[30] K. A. Smith, "The quantal theory of how the immune system discriminates between 'self and non-self,'" *Med. Immunol.*, vol. 3, pp. 1–22, Jan. 2004.

[31] E. L. Cooper, "Evolution of immune systems from self/not self to danger to artificial immune systems (AIS)," *Phys. Life Rev.*, vol. 7, no. 1, pp. 55–78, Mar. 2010.

[32] P. Matzinger, "The evolution of the danger theory," *Expert Rev. Clin. Immunol.*, vol. 8, no. 4, pp. 311–317, May 2012.

[33] P. Matzinger, "Tolerance, danger, and the extended family," *Annu. Rev. Immunol.*, vol. 12, no. 1, pp. 991–1045, Apr. 1994.

[34] J. McNiff and J. Whitehead, "Danger theory," in *Action Research in Organisations*. Evanston, IL, USA: Routledge, 2002, pp. 95–110.

[35] P. Matzinger, "Essay 1: The danger model in its historical context," *Scandin. J. Immunol.*, vol. 54, nos. 1–2, pp. 4–9, Jul. 2001.

[36] L. N. de Castro and F. J. Von Zuben, "Learning and optimization using the clonal selection principle," *IEEE Trans. Evol. Comput.*, vol. 6, no. 3, pp. 239–251, Jun. 2002.

[37] L. N. De Castro and J. Timmis, *Artificial Immune Systems: A New Computational Intelligence Approach*. Cham, Switzerland: Springer, 2002.

[38] U. Aickelin and S. Cayzer, "The danger theory and its application to artificial immune systems," 2008, *arXiv:0801.3549*.

[39] S. Wang, Y. C. Liang, W. D. Li, and X. T. Cai, "Big data enabled intelligent immune system for energy efficient manufacturing management," *J. Cleaner Prod.*, vol. 195, pp. 507–520, Sep. 2018.

[40] J. Timmis and M. Neal, "A resource limited artificial immune system for data analysis," *Knowl.-Based Syst.*, vol. 14, nos. 3–4, pp. 121–130, Jun. 2001.

[41] O. Nasraoui, D. Dasgupta, and F. A. González, "An novel artificial immune system approach to robust data mining," in *Proc. GECCO Late Breaking Papers*, 2002, pp. 356–363.

[42] J. Brown, M. Anwar, and G. Dozier, "An artificial immunity approach to malware detection in a mobile platform," *EURASIP J. Inf. Secur.*, vol. 2017, no. 1, pp. 1–10, Dec. 2017.

[43] J. Brown, M. Anwar, and G. Dozier, "Detection of mobile malware: An artificial immunity approach," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2016, pp. 74–80.

[44] V. Golovko, S. Bezobrazov, P. Kachurka, and L. Vaitsekhovich, "Neural network and artificial immune systems for malware and network intrusion detection," in *Advances in Machine Learning II*. Cham, Switzerland: Springer, 2010, pp. 485–513.

[45] D. Dasgupta, "Artificial neural networks and artificial immune systems: Similarities and differences," in *Proc. IEEE Int. Conf. Syst., Man, Cybern., Comput. Cybern. Simulation*, vol. 1, 1997, pp. 873–878.

[46] M. B. A. Hamid and T. K. A. Rahman, "Short term load forecasting using an artificial neural network trained by artificial immune system learning algorithm," in *Proc. 12th Int. Conf. Comput. Model. Simul.*, Mar. 2010, pp. 408–413.
[47] Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Cost of Cyber Incidents Study*. Accessed: Jun. 16, 2023.
[48] C. R. Sunstein, "Cost-benefit analysis and the environment," *Ethics*, vol. 115, no. 2, pp. 351–385, 2005.
[49] E. J. Mishan and E. Quah, *Cost-benefit Analysis*. Evanston, IL, USA: Routledge, 2020.
[50] J. A. Annema, N. Mouter, and J. Razaei, "Cost-benefit analysis (CBA), or multi-criteria decision-making (MCDM) or both: Politicians' perspective in transport policy appraisal," *Transp. Res. Proc.*, vol. 10, pp. 788–797, Jan. 2015.
[51] C. Koopmans and N. Mouter, *Cost-Benefit Analysis* (Advances in Transport Policy and Planning), vol. 6. Amsterdam, The Netherlands: Elsevier, 2020, pp. 1–42.
[52] D. Mugo, K. Njagi, B. Chemwei, and J. Motanya, "The technology acceptance model (TAM) and its application to the utilization of mobile learning technologies," *Brit. J. Math. Comput. Sci.*, vol. 20, no. 4, pp. 1–8, Jan. 2017.
[53] F. D. Davis, A. Granić, and N. Marangunić, "The technology acceptance model 30 years of tam," *Technology*, vol. 1, no. 1, pp. 1–150, 2023.
[54] S. L. ToralMarin, F. J. BarreroGarcia, R. MartinezTorres, S. GallardoVazquez, and A. J. LilloMoreno, "Implementation of a web-based educational tool for digital signal processing teaching using the technological acceptance model," *IEEE Trans. Educ.*, vol. 48, no. 4, pp. 632–641, Nov. 2005.
[55] X. Hu, M. A. Griffin, and M. Bertuleit, "Modelling antecedents of safety compliance: Incorporating theory from the technological acceptance model," *Saf. Sci.*, vol. 87, pp. 292–298, Aug. 2016.
[56] W. J. Potter and D. Levine-Donnerstein, "Rethinking validity and reliability in content analysis," *J. Appl. Commun. Res.*, vol. 27, no. 3, pp. 258–284, Aug. 1999.
[57] F. L. Schmidt, C. Viswesvaran, and D. S. Ones, "Reliability is not validity and validity is not reliability," *Personnel Psychol.*, vol. 53, no. 4, pp. 901–912, 2000.
[58] E. Oz, "Ethical standards for information systems professionals: A case for a unified code," *MIS Quart.*, vol. 16, no. 4, p. 423, Dec. 1992.
[59] D. Wright, "A framework for the ethical impact assessment of information technology," *Ethics Inf. Technol.*, vol. 13, no. 3, pp. 199–226, Sep. 2011.
[60] H. Xu, T. Dinev, J. Smith, M. University, and P. Hart, "Information privacy concerns: Linking individual perceptions with institutional privacy assurances," *J. Assoc. Inf. Syst.*, vol. 12, no. 12, pp. 798–824, Dec. 2011.
[61] D. Kelley and K. Atreides, "AGI protocol for the ethical treatment of artificial general intelligence systems," *Proc. Comput. Sci.*, vol. 169, pp. 501–506, Jan. 2020.

OLUFUNSHO I. FALOWO received the B.A. degree in philosophy from the University of Lagos, Nigeria, in 2004, and the M.B.A. degree from the Isenberg School of Management, University of Massachusetts, in 2021. He is currently pursuing the Ph.D. degree in information technology with the School of Information Technology, University of Cincinnati, Cincinnati, OH, USA. His research interests include cloud security, security information and event management, security incident detection and response, ethical computer hacking, and digital forensic investigation among others. He is also a member of the International Information System Security Certification Consortium and the Information Systems Audit and Control Association. In 2021, he completed an executive education in Design Thinking: A toolkit for Breakthrough Innovation with the Kellogg School of Management, Northwestern University. In 2022, he completed an executive education in Cybersecurity: Managing Risks in The Information Age at Harvard University. He completed an executive education in Behavioral Economics at The University of Chicago Booth School of Business, in 2022. He completed an executive education in Negotiation Strategies at The Yale School of Management, in 2022. Also completed an executive education in Building Resilience and Agility at The London Business School, in 2022. He has been a Certified Information Systems Security Professional, since 2017, a Certified Information Security Manager, since 2020, a Certified Computer Hacking Forensic Investigator, since 2011, and a Certified Security Analyst, since 2010. Also a certified ISO/IEC 27001:2005 Lead Implementer.

LILY EDINAM BOTSYOE is currently pursuing the Ph.D. degree in information technology, is part of UC's inaugural Presidential Fellowship Program, and a former Adjunct Instructor. She is an ardent contributor to technology communities and speaks widely on issues relating to the internet with a particular interest in Women and Youth Inclusion, Accessibility, Cybersecurity, Privacy, and Digital Sustainability. She has experience working with security frameworks and regulations, such as GDPR, ISO27001, NIST 800, HIPAA, and PCI DSS. As a believer in the power of technology to accelerate development, her work focuses on human-centered approaches to building technology that ignites real impact for users. She grounds her strategies in the principles of digital inclusion and solutions focused on sustainability and scale. In the Internet Governance and policy space, she coordinates the Ghana Youth Internet Governance Forum and is a member of the steering committee for West Africa and Africa Youth Internet Governance Forum. She is part of the 30 women awarded the STEM Woman Honour 2020 at the National Women in STEM Honour in Ghana for her contribution to the field of work and education under STEM. This has spurred her interest to start a book-based mentorship to build a STEM Identity for girls through a color book. She was also awarded the 2021 Research and Knowledge Builder in Ghana by the Coalition for Digital Equality. Outside the above listed, she hosts a weekly podcast called Pointers in ten which shares nuggets on tech, digital leadership, career, and personal branding.

KEHINDE KOSHOEDO received the B.Sc. (ED) degree in mathematics from the University of Lagos, Nigeria, in 2004, the M.Sc. degree from the Infrastructure Planning and Development from Oxford Brookes University, U.K., and the M.B.A. degree in hyperconnectivity from Nexford University, Washington. He is currently pursuing the Ph.D. degree with Oxford Brookes University, U.K. He is the Chief Risk Officer of ARM Pension, Nigeria's second-largest Pension Fund Administrator (PFA) with over $2b billion in assets under management. He is an Expert in Enterprise Risk Management and Governance with more than 15 years of work experience in financial services working across various areas of risk management that include technology, operational, compliance, financial risk, and governance.

MURAT OZER received the M.S. degree in public administration from the Public Administration Institute for Turkey and the Middle East, Ankara, in 2006, and the M.S. and Ph.D. degrees in criminal justice from the University of Cincinnati, in 2007 and 2010. He is currently an Associate Professor with the School of Information Technology. His primary research interests include crime information to generate predictive data analytics for various public health problems, such as drug-related problems, street violence, and cybersecurity. He works with law enforcement and correction agencies in the nation and develops certain web-based predictive analytical systems.