GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN IN PUBLICA COMMODA SEIT 1737

HPS

Seminar Report

Security in Cloud and HPC

Michael Hubert Duah

MatrNr: 11710452

Supervisor: Trevor Khwam

Georg-August-Universität Göttingen
Institute of Computer Science

March 31, 2024

Abstract

In the era of digital transformation, High-Performance Computing (HPC) and Cloud environments have emerged as critical enablers of data-intensive applications and cutting-edge research across various domains. However, the immense computational power and vast data repositories inherent to these systems also present significant security challenges. This report delves into the intricate landscape of cybersecurity in HPC and Cloud environments, exploring the limitations of traditional security measures and proposing innovative solutions that leverage the synergistic potential of Artificial Intelligence (AI) and HPC technologies. Through a comprehensive analysis, this study illuminates the unique security requirements and constraints of HPC and Cloud systems, highlighting the need for proactive, adaptive, and scalable defense mechanisms. The integration of AI and machine learning techniques with HPC's computational capabilities is presented as a pivotal strategy to combat the ever-evolving sophistication of cyber threats. Furthermore, this report emphasizes the importance of a holistic approach to cybersecurity, encompassing technological advancements, human capital development, and collaborative efforts underpinned by proactive policy frameworks. It underscores the necessity of cultivating a cybersecurity-aware culture, fostering multidisciplinary research and development, and promoting responsible AI adoption guided by ethical principles of privacy, fairness, and transparency. Ultimately, this study contributes to the ongoing discourse on enhancing cybersecurity resilience in high-performance computing ecosystems, advocating for the development of a vibrant cybersecurity ecosystem that harmonizes technological innovation, human expertise, and adaptive governance. By exploring the convergence of HPC and AI, this report paves the way for intelligent, adaptive, and collaborative security solutions capable of safeguarding the digital fortresses of the future.

Declaration on the use of ChatGPT and comparable tools in the context of examinations

In this work I have used ChatGPT or another AI as follows:

- ☐ Not at all
- ☐ During brainstorming
- ☐ When creating the outline
- ☐ To write individual passages, altogether to the extent of 0% of the entire text
- ☐ For the development of software source texts
- ☑ For optimizing or restructuring software source texts
- ☑ For proofreading or optimizing
- ☐ Further, namely: -

I hereby declare that I have stated all uses completely.
Missing or incorrect information will be considered as an attempt to cheat.

Contents

1 Introduction

In the realm of High-Performance Computing (HPC) and Cloud environments, ensuring robust security measures is paramount to safeguarding sensitive data and critical infrastructure. The paper delves into the intricate landscape of cybersecurity within these advanced computing systems, shedding light on the challenges, innovations, and solutions that shape the evolving domain of digital protection.

As technology continues to advance at a rapid pace, the need for sophisticated security mechanisms in HPC and Cloud settings becomes increasingly pressing. The intersection of artificial intelligence, data analytics, and traditional security measures presents a dynamic landscape where novel approaches are essential to fortify defenses against ever-evolving cyber threats.

Through a comprehensive exploration of the current state of security in Cloud and HPC environments, this report navigates the complexities of safeguarding data integrity, confidentiality, and availability in the face of sophisticated cyber adversaries. By examining the limitations of existing security frameworks and proposing innovative solutions that leverage cutting-edge technologies, this research contributes to the ongoing discourse on enhancing cybersecurity resilience in high-performance computing ecosystems.

With a focus on collaborative intelligence, the integration of AI with traditional security measures, and the imperative of human-machine teaming, this report underscores the multifaceted nature of cybersecurity in modern computing landscapes. By emphasizing the importance of a holistic approach that encompasses people, processes, and technology, this study advocates for a synergistic fusion of human expertise and technological innovation to fortify the digital fortresses of Cloud and HPC systems.

In the following sections, we delve deeper into the challenges faced by security practitioners in HPC and Cloud environments, explore the innovative solutions proposed to address these challenges, and reflect on the implications of these advancements for the future of cybersecurity in high-performance computing.

2 Security Challenges in HPC systems

High-performance computing (HPC) systems present unique security challenges due to their scale, complexity, and high-speed data processing capabilities. [Pei17] highlights that the interconnected nature of HPC environments makes them susceptible to various cyber threats, ranging from unauthorized access to data breaches. One prominent challenge is the vulnerabilities present in the network infrastructure of HPC systems. [Yan+21] emphasize the importance of protecting the network architecture from external attacks and internal breaches, given the critical role of network connectivity in HPC operations. Protecting sensitive data and ensuring privacy are significant challenges in HPC environments. [Che23] discusses the importance of confidentiality in HPC, especially when dealing with sensitive research data or proprietary information. Unauthorized access to data can lead to intellectual property theft or privacy violations. Maintaining robust authentication mechanisms and access control policies is essential in HPC systems to prevent unauthorized users from accessing resources. [AZM23] highlight the challenges associated with implementing effective authentication protocols and access controls in cloud-based HPC environments. Effective resource management and allocation pose challenges in

HPC systems, particularly in multi-tenant environments where multiple users share resources. [EEH22] discuss the need for efficient resource scheduling algorithms and policies to prevent resource contention and optimize performance while ensuring security. HPC systems are vulnerable to insider threats, where authorized users misuse their privileges to compromise system integrity or steal sensitive data. [II18] emphasize the importance of monitoring user activities and implementing insider threat detection mechanisms to mitigate such risks. The complexity of software stacks and dependencies in HPC applications increases the likelihood of software vulnerabilities and exploits. [Osm+23] discuss the challenges associated with patch management and software updates in cloud-based HPC environments to address security vulnerabilities effectively. HPC systems often rely on distributed computing architectures, introducing additional security challenges related to communication and coordination among distributed components. [JL23] discuss the need for secure communication protocols and encryption mechanisms to protect data transmitted between distributed nodes. Physical security risks, such as tampering with hardware components or unauthorized access to data centers, pose significant threats to HPC systems. [MPK23] highlight the importance of implementing robust physical security measures, including surveillance, access controls, and environmental monitoring, to safeguard HPC infrastructure. HPC systems face the challenge of dealing with emerging threats and evolving attack vectors, such as advanced persistent threats (APTs), ransomware, and zero-day exploits. [Abd23] discusses the importance of threat intelligence and proactive defense strategies to detect and mitigate these evolving threats effectively.

Security challenges in HPC systems encompass many issues, including network vulnerabilities, data security concerns, authentication and access control, insider threats, software vulnerabilities, distributed computing security, physical security risks, and emerging threats. Addressing these challenges requires a comprehensive approach that integrates technical solutions, policy frameworks, and proactive defense strategies to protect HPC infrastructure and data assets.

3 Artificial Intelligence Techniques for Cybersecurity in HPC

The urgency for advanced cybersecurity measures intensifies as cyber threats increase in frequency and sophistication, while digital expansion persists unchecked. This scenario necessitates a paradigm shift in cybersecurity strategies due to the convergence of factors straining traditional security approaches [Tha24] Hyperconnectivity fuels the proliferation of digital endpoints and systems, escalating the average cost of data breaches. Moreover, the rapid digital transformation, driven by technologies like cloud computing, mobile devices, IoT, and AI, surpasses organizations' ability to secure their infrastructure, leading to a dynamically changing threat landscape [NDT24]

Geopolitical dynamics further compound challenges, with state-sponsored cyber warfare capabilities increasingly deployed by nation-states. Instances such as the Russia-Ukraine conflict witness large-scale cyberattacks, highlighting the convergence of geopolitical tensions and cyber threats. Additionally, cybercrime growth, facilitated by online anonymity and sophisticated hacking tools, poses significant challenges. The rise of cryptocurrencies further emboldens cybercriminals, enabling untraceable transactions. Moreover, disinformation weaponization through social engineering and phishing exacerbates

cybersecurity risks, amid a critical shortage of cybersecurity expertise [SLF23]. Conventional security approaches have proven inadequate against emerging threats. Signature-based detection methods are ineffective against zero-day exploits, and siloed security monitoring leads to slow response times. Compliance audits and vulnerability assessments often fail to address dynamic risks, leaving organizations vulnerable to new threats. Password-based authentication schemes remain susceptible to attacks, highlighting the need for a cybersecurity transformation [MK23]. High-Performance Computing (HPC) and Artificial Intelligence (AI) offer promise in revolutionizing cybersecurity by enabling proactive and adaptive defense mechanisms. HPC's computing capabilities facilitate scaling up AI-based security solutions, optimizing them to address rapidly evolving threats and ushering in a new era of cybersecurity resilience and effectiveness.

3.1 High-Performance Computing (HPC)

High-performance computing (HPC) represents a sophisticated approach to aggregating computer resources to achieve significantly higher performance levels than those typically achievable with desktop computers [Hoe+24]. HPC systems are characterized by their utilization of specialized hardware components, such as accelerators, combined with high-speed interconnects, all managed through optimized software stacks. Key features of HPC systems include the deployment of distributed supercomputing clusters comprising thousands of nodes, capable of delivering petaflops of processing power [CH24]. Additionally, these systems leverage diverse accelerators like GPUs, TPUs, and FPGAs to expedite parallel workloads, while employing low latency networks such as Infiniband and Omni-Path to facilitate rapid intra-cluster communication [PJ24]. Furthermore, HPC systems are supported by optimized operating systems, databases, libraries, and tools, along with workload managers and schedulers that facilitate resource allocation and job automation [NLS23]. The architecture of HPC systems is designed to be modular and scalable, ranging from cloud-based implementations to supercomputers like the Exascale Frontier system [Gil+24].

This combination of hardware, software, and networking components enables HPC systems to provide the massive throughput and low-latency access to memory and storage required by modern data-intensive applications. HPC plays a pivotal role in facilitating cutting-edge research across various scientific and engineering disciplines, including physics, astronomy, genomics, and material science [PJ24]. Moreover, HPC systems are indispensable for conducting real-time analytics of massive datasets generated by instruments and sensors, as observed in domains like the Internet of Things (IoT), smart infrastructure, and financial services [Aja+24]. As cloud-hosted HPC solutions become increasingly accessible to mainstream enterprises, the scope of its applications in the realm of cybersecurity is expanding.

3.2 Artificial Intelligence (AI)

Artificial intelligence (AI) encompasses computational techniques that empower systems to execute tasks typically requiring human cognition and perception [Ped24]. Leveraging learning from data, AI systems possess the capability to continuously enhance their performance through experience. Core AI methodologies include machine learning, which employs algorithms such as neural networks to learn from data without explicit programming, and deep learning, which enhances multi-layer neural networks to discern complex

patterns effectively [KA23]. Additionally, reinforcement learning optimizes actions by maximizing rewards through trial-and-error [Tym+23], while computer vision processes and analyzes visual data using deep neural networks. Moreover, natural language processing facilitates the interpretation of text and speech data, and generative models like Generative Adversarial Networks (GANs) are employed to create synthetic data [KA23]. When combined with big data and substantial computing power, AI has demonstrated superhuman performance in specialized tasks ranging from playing games and generating art to language translation and medical diagnosis [KTW23].

Extending AI's capabilities to the realm of cybersecurity represents a natural strategic imperative to keep pace with exponentially growing data volumes and increasing attack sophistication. Various key applications of AI in cybersecurity include predictive threat modeling [Geo24], intelligent deception strategies [Ghe], user and entity behavior analytics (UEBA) [MS], adaptive access controls, automated threat intelligence, and rapid malware analysis at scale [KA23].

3.3 The Convergence of HPC and AI in Cybersecurity

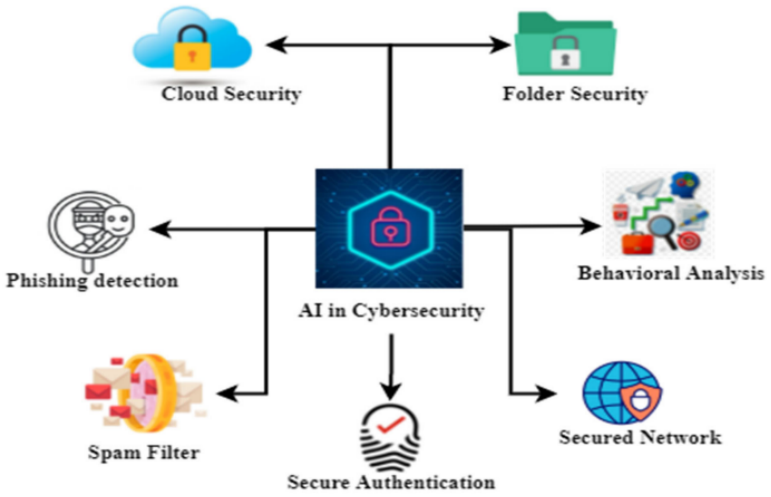

Figure 1: AI in Cybersecurity.

These diverse applications underscore the expanding potential of AI in enhancing cybersecurity defenses. However, realizing the full potential of AI in cybersecurity necessitates ample training data and computing power, areas in which high-performance computing (HPC) systems play a pivotal role. Through the convergence of AI and HPC technologies 1, organizations can harness the transformative power of intelligent and adaptive cybersecurity solutions to effectively combat evolving cyber threats.

By combining high-performance computing (HPC) and artificial intelligence (AI), powerful new cybersecurity capabilities become possible [MK23]. Some notable use cases are:

Scalable Threat Detection

Analyzing massive volumes of security data like logs, network packets, and alerts in real time is crucial for timely threat detection. However, this data can easily overwhelm traditional systems [ALS23]. HPC enables the processing of billions of these events daily to uncover anomalies and threats faster. For example, Sandia National Labs uses an HPC

cluster for high-speed intrusion detection, analyzing 75 billion network packets per second, revealing stealthy threats missed by legacy tools [Vel24]. Integrating big data analytics with AI/machine learning techniques further enhances this capability by modeling normal versus abnormal behaviors and enabling forensics [JTS]. Such solutions help transition security operations centers into proactive defense centers.

Security Model Development
Developing robust machine learning-based security models requires vast amounts of labeled data covering diverse attack scenarios and system behaviors [Lea+23]. HPC-accelerated simulation and synthetic data generation enable creating this data at scale. DARPA's Cyber Grand Challenge used supercomputers to create AI systems that could automatically detect, analyze, and patch software vulnerabilities [ASA24]. Training such complex models through HPC-powered simulation opens new frontiers in cyber defense.

Threat Intelligence and Prediction
Threat intelligence involves understanding adversaries' tactics, tools, and motives [LZ24]. AI excels at aggregating and correlating threat data from multiple sources to gain situational awareness and predict future adversary moves. Los Alamos National Laboratory is pursuing cyber threat intelligence leveraging graph analytics combined with machine learning on security event datasets to inform threat modeling, risk metrics, and mitigation priorities [Rob24].

Open-Source Intelligence (OSINT)
The internet contains a wealth of public data for understanding threat actors and campaigns. AI helps synthesize intelligence from this unstructured data across social media, code repositories, forums, etc [Dey23]. Researchers have demonstrated using machine learning to analyze billions of GitHub repositories for cryptographic weaknesses and vulnerable code [Fu+23]. Such OSINT methods, powered by HPC and AI, uncover threat signals missed by other means.

Collaborative Defense
Cyber risks transcend organizational boundaries, necessitating collective security efforts. However, sharing proprietary data to train AI models raises confidentiality concerns. Federated Learning (FL) addresses this by enabling collaborative model training without data exchange [Yan+21]. Different entities train models locally using their own data, sharing only model updates while preserving privacy. HPC makes the computationally intensive FL approach practical, and it has been explored for use cases like threat classification, fraud detection, and malware analytics [Cor]. The synergy of FL with HPC-AI merits further exploration for strengthening collective cyber defenses.

While promising, technology alone is insufficient. Maximizing the effectiveness of HPC-AI in cybersecurity requires an integrated focus on people and processes as well [MK23].

3.4 Integration of AI with Traditional Security Measures

Traditional IT security solutions like network and host-based intrusion detection, access controls, and software verification often perform poorly in high-performance computing (HPC) environments due to constraints [Pei17]. For instance, certain network security

mechanisms like firewalls doing deep packet inspection can be detrimental to HPC systems' performance needs. Even a minuscule 0.0046% packet loss can cause a 90% drop in network data transfer throughput [con23].

Alternative approaches tailored to HPC environments must be applied. The Science DMZ security framework defines policies, procedures, and mechanisms addressing the distinct needs of scientific computing with high throughput requirements [Veg+24]. It isolates scientific systems in an enclave separate from other computing systems with different security needs. Network transfers are directed through a single ingress/egress point for monitoring and restriction.

However, instead of deep packet inspection or stateful firewalls that could impede throughput, the Science DMZ leverages packet filtering firewalls examining only packet headers, not payloads [con23]. Deep packet inspection and stateful intrusion detection are performed separately, not inline with traffic, to avoid transmission delays and congestion [Pei17].

By centralizing monitoring at this single point, the framework aims to maintain security levels similar to traditional organizations with a single ingress/egress, but accommodating the traffic volume and type in HPC environments [Veg+24]. Reducing complexity to achieve throughput is a key theme.

The widely adopted Science DMZ framework, funded by NSF and DOE, supports open science computing infrastructure but must continue adapting to environments with stricter confidentiality needs like medical, defense and intelligence contexts [Pei17]. Steps have been taken for medical environments through the Medical Science DMZ applying the framework for HIPAA compliance, but further work across domains is required [Veg+24].

Artificial Intelligence (AI) can complement traditional security measures in High-Performance Computing (HPC) systems by addressing the unique challenges and constraints of these environments. Traditional security solutions, such as network and host-based intrusion detection, access controls, and software verification, often perform poorly in HPC environments due to the high throughput and low-latency requirements [Pei17] For instance, deep packet inspection firewalls can introduce delays that lead to packet loss and a significant drop in network data transfer throughput [con23]

AI-based security approaches can provide more effective and efficient solutions tailored to the distinct needs of HPC systems. Machine learning techniques can be employed for anomaly detection and behavior analysis, leveraging the vast amounts of data generated by HPC systems [PJ24]. By modeling normal system behavior, AI algorithms can identify deviations and potential threats in real-time, without imposing significant performance overhead [CBK09].

Furthermore, AI can enhance threat intelligence and prediction capabilities in HPC environments. Graph analytics combined with machine learning can be applied to security event datasets to gain insights into adversaries' tactics, tools, and motives [Rob24]. This intelligence can inform threat modeling, risk metrics, and mitigation priorities, enabling proactive defense strategies [Jaj+16].

Open-Source Intelligence (OSINT) is another area where AI can complement traditional security measures in HPC systems. Machine learning techniques can be employed to analyze vast amounts of public data, such as code repositories, social media forums, and online discussions, to uncover potential vulnerabilities, threat actors, and campaigns [Wu20; Dey23]. This intelligence can be integrated with other security data to provide a comprehensive view of the threat landscape.

Moreover, AI can facilitate collaborative defense efforts in HPC environments. Feder-

ated Learning (FL) enables collaborative model training without data exchange, addressing confidentiality concerns [Yan+19]. Different organizations can train AI models locally using their data and share only model updates, preserving privacy. High-Performance Computing (HPC) systems make the computationally intensive FL approach practical, enabling collective threat classification, fraud detection, and malware analytics [Cor].

While AI offers promising solutions, it is essential to recognize that technology alone is insufficient. Maximizing the effectiveness of AI in HPC security requires an integrated focus on people, processes, and technology [PJ24]. Collaboration between domain experts, security professionals, and AI researchers is crucial for developing robust and context-aware AI-based security solutions for HPC environments.

3.5 The Human Factor: Collaborative Intelligence

Cybersecurity is ultimately about enabling people to use technology safely, and human-machine teaming is crucial for developing robust solutions. Artificial Intelligence (AI) and automation are force multipliers, but not replacements for human intelligence. Combining their complementary strengths fosters collaborative intelligence [PJ24]. Some guiding principles include:

Augmenting Human Analysts
Threat analysts today struggle with information overload, but their judgment, reasoning, and response capabilities remain indispensable. AI is best leveraged to assist human analysts rather than replace them. Explainable AI models empower analysts to focus on high-value inferences rather than raw data. Contextual performance metrics should emphasize enhanced productivity over automation rate [Raw+21]).

Cooperative Advantage
Neither humans nor machines are foolproof. AI models have blindspots and can be deceived. However, together they exhibit cooperative advantage, becoming more than the sum of their parts. Human-machine teams must be designed for agility, safety, and trust. Keeping the human in the loop, especially for high-risk actions, is advised [Jia+20].

Ethical & Responsible AI
As AI permeates security systems, ethical risks like privacy infringement, bias, and overreach heighten. Transparent and accountable AI guided by principles of non-maleficence is vital. Fostering public awareness of AI use cases while addressing concerns through stakeholder engagement builds further trust [Jia+20].

Holistic Cyber Risk Management
Beyond core IT systems, the human element significantly influences cyber risks via phishing, social engineering, or accidental breaches. Awareness education, along with cyber hygiene and resilience policies for the extended enterprise, are key mitigation strategies. Cyber risk must be managed holistically across technical, human, and organizational spheres [SVF16].

Adaptive Policy Framework
Cybersecurity policies and regulations shape risk management practices and incentives. However, static policies struggle to keep pace with technology and threat evolution. Policy

frameworks must be designed for adaptation based on empirical feedback, much like cyberdefenses. Agile governance is needed to spur innovation while ensuring safety, similar to aviation regulation [Zha+22].

4 Recommendations

Addressing modern cyber risks at scale requires a concerted effort to develop advanced computational capabilities, nurture human capital, and foster collaborative solutions, underpinned by proactive policy efforts [MK23]. Some recommendations in these dimensions are:

Multidisciplinary Research and Development in Cybersecurity
Cybersecurity is an inherently multidisciplinary field, necessitating an integrated approach to research and development (R&D) that spans computer science, engineering, social sciences, policy, law, and the humanities[All]. This broad collaboration is essential to tackle the complex and evolving challenges of securing digital infrastructures and information. Key directions include developing machine learning technologies that are not only efficient but also resilient to attacks and biases, applying advanced mathematics to create secure and privacy-preserving computational frameworks, designing specialized hardware for enhanced security capabilities, integrating usable security principles into human-centered systems, and conducting economic, behavioral, and risk analysis modeling to inform policy-making processes [SP10]. Establishing standards for safety, ethics, and algorithmic accountability is crucial, as is funding mission-driven, use-inspired research that balances long-term knowledge generation with practical near-term prototyping [Her23]. Promoting open collaboration platforms that connect industry, academia, and government is vital for broader adoption and integration. Ultimately, creating a thriving cybersecurity innovation ecosystem requires a comprehensive approach that integrates research across disciplines, sectors, and the entire research pipeline, from foundational studies to implementation strategies [Jaj+16].

Education and Skills Development
Growing the talent pipeline at all levels is imperative, spanning K-12 STEM and cyber ethics education, university-level training in core competencies like secure coding and cryptographic engineering, and workplace reskilling programs on changing toolsets. Multidisciplinary degrees combining computer science with law, criminal justice, or public policy foster wider perspectives. Apprenticeship programs and cyber ranges offer hands-on learning, while outreach efforts, competitions, and certifications help signal competencies and close the cyber skills gap.

Responsible Development
The advancement of High-Performance Computing and Artificial Intelligence (HPC-AI) security must be pursued within a framework of social responsibility, ensuring that technological progress does not come at the expense of ethical standards or societal well-being. Key principles include privacy, fairness, and safety in system design, promoting incentives for cyber hygiene and securing the human element, ensuring transparency and auditability of algorithms to build trust, assessing the impact of automation on human workers and the need for oversight, and engaging in proactive policy and ethics dialogues with diverse

stakeholders, including industry experts, policymakers, and the public.
While voluntary adoption of norms and ethical codes of conduct is important, it should be supplemented by binding regulations where necessary to ensure compliance and protect public interests. This dual approach encourages innovation and responsible behavior within the industry while providing a safety net through regulatory oversight. The goal of responsible development in HPC-AI security is to enhance cybersecurity capabilities prudently and ethically, ensuring that technological advances contribute positively to society and do not exacerbate existing inequalities or introduce new risks.

Multilateral Collaboration
Cyber risks being borderless necessitates global cooperation and collective response. Beyond technology standards, this requires multilateral treaties against cyberwarfare, intelligence-sharing arrangements, and joint training exercises. Coordinated vulnerability disclosure policies and bug bounty programs with industry participation also help strengthen defense. Combating cybercrime requires harmonizing laws, investigative protocols, and enforcement jurisdictions across nations.

Adaptive Governance
Policies and regulations shape risk management practices and business incentives. However, static policies struggle to respond to rapidly changing threats and technologies. Cyber governance needs to become more empirically driven and nimble, able to dynamically adapt policies based on evidence and experience, much like the systems being regulated. This entails systematic feedback loops, sandboxing of emerging capabilities, and close public-private coordination.

With a concerted push across these dimensions, the synergistic potential of HPC and AI can be realized for significantly enhancing cybersecurity and resilience. However, technology is only one piece of the puzzle – fostering a vibrant cybersecurity ecosystem requires a whole-of-society approach.

5 Conclusion

Through a comprehensive analysis of the challenges, innovations, and solutions in securing Cloud and HPC environments, this report underscores the imperative of proactive defense strategies and adaptive security frameworks to mitigate emerging cyber threats effectively.

As technology continues to advance and cyber adversaries grow increasingly sophisticated, the integration of artificial intelligence, machine learning, and big data analytics emerges as a pivotal strategy in fortifying the resilience of Cloud and HPC systems against malicious actors. By harnessing the power of high-performance computing to accelerate threat detection, anomaly identification, and predictive analytics, organizations can enhance their cybersecurity posture and transition from reactive to proactive defense mechanisms.

The convergence of HPC and AI heralds a transformative era for cybersecurity, promising to elevate our defenses against the backdrop of hyper-connectivity and the escalating threat environment we face today. However, technology alone will not suffice to address the multifaceted challenges posed by cyber threats. A systemic approach that encompasses technological, human, and policy dimensions is essential for maximizing the impact of this synergistic innovation.

Moreover, the report emphasizes the importance of collaboration, both between human experts and intelligent systems, and across diverse domains to leverage threat intelligence, open-source data, and innovative security models. By fostering a culture of information sharing, continuous learning, and adaptive response, stakeholders in the Cloud and HPC ecosystem can collectively strengthen their defenses and stay ahead of evolving cyber threats.

The ethical implications of deploying AI in cybersecurity cannot be overstated, necessitating a framework that balances innovation with accountability, transparency, and respect for privacy. As AI systems become increasingly autonomous, establishing mechanisms for ethical oversight and ensuring that these systems operate within defined moral and legal boundaries is essential. This includes the development of international standards and norms that guide the responsible use of AI in cybersecurity, promoting a unified approach to tackling global cyber threats.

Looking ahead, the insights and recommendations presented in this report serve as a foundation for further research, innovation, and collaboration in the field of cybersecurity for high-performance computing. By embracing a holistic approach that integrates technical solutions, policy frameworks, and human expertise, organizations can navigate the complex cybersecurity landscape with resilience, agility, and foresight.

References

[Abd23] Fargana Abdullayeva. "Cyber resilience and cyber security issues of intelligent cloud computing systems". In: *Results in Control and Optimization* 12 (2023), p. 100268.

[Aja+24] Samir N Ajani et al. "Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing". In: *International Journal of Intelligent Systems and Applications in Engineering* 12.7s (2024), pp. 546–559.

[All] Cloud Security Alliance. *High Performance Computing*. URL: `https://cloudsecurityalli` `org/research/topics/high-performance-computing-cloud-security`.

[ALS23] Giovanni Apruzzese, Pavel Laskov, and Johannes Schneider. "SoK: Pragmatic assessment of machine learning for network intrusion detection". In: *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. IEEE. 2023, pp. 592–614.

[ASA24] Mohd Firdaus bin Abas, Balbir Singh, and Kamarul Arifin Ahmad. "High Performance Computing and Its Application in Computational Biomimetics". In: *High Performance Computing in Biomimetics: Modeling, Architecture and Applications*. Springer, 2024, pp. 21–46.

[AZM23] Hussain Akbar, Muhammad Zubair, and Muhammad Shairoze Malik. "The security issues and challenges in cloud computing". In: *International Journal for Electronic Crime Investigation* 7.1 (2023), pp. 13–32.

[CBK09] Varun Chandola, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey". In: *ACM computing surveys (CSUR)* 41.3 (2009), pp. 1–58.

[CH24] Diane Coyle and Lucy Hampton. "21st century progress in computing". In: *Telecommunications Policy* 48.1 (2024), p. 102649.

[Che23] Keke Chen. "Confidential High-Performance Computing in the Public Cloud". In: *IEEE Internet Computing* 27.1 (2023), pp. 24–32.

[con23] Wikipedia contributors. *Science DMZ Network Architecture*. Oct. 2023. URL: `https://en.wikipedia.org/wiki/Science_DMZ_Network_Architecture#Components`.

[Cor] Nvidia Corporation. *HPC AI in action*. URL: `https://www.nvidia.com/en-us/high-performance-computing/hpc-and-ai/`.

[Dey23] Victor Dey. "How high-performance computing at the edge fuels AI, AR/VR, cybersecurity and more". In: *VentureBeat* (July 2023). URL: `https://venturebeat.com/ai/how-high-performance-computing-at-the-edge-is-reshaping-data-center-intelligence/`.

[EEH22] Said El Kafhali, Iman El Mir, and Mohamed Hanini. "Security threats, defense mechanisms, challenges, and future directions in cloud computing". In: *Archives of Computational Methods in Engineering* 29.1 (2022), pp. 223–246.

[Fu+23] Yujia Fu et al. "Security Weaknesses of Copilot Generated Code in GitHub". In: *arXiv preprint arXiv:2310.02059* (2023).

[Geo24] A Shaji George. "Riding the AI Waves: An Analysis of Artificial Intelligence's Evolving Role in Combating Cyber Threats". In: *Partners Universal International Innovation Journal* 2.1 (2024), pp. 39–50.

[Ghe] Diptiben Ghelani. "Securing the Future: Exploring the Convergence of Cybersecurity, Artificial Intelligence, and Advanced Technology". In: ().

[Gil+24] Sukhpal Singh Gill et al. "Modern computing: Vision and challenges". In: *Telematics and Informatics Reports* (2024), p. 100116.

[Her23] Taylor Hersom. *The Cyber Risks of scaling: How to secure your expanding attack surfaces*. en-US. Feb. 2023. URL: https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/the-cyber-risks-of-scaling-how-to-secure-expanding-attack-surfaces/amp/.

[Hoe+24] Torsten Hoefler et al. "XaaS: Acceleration as a Service to Enable Productive High-Performance Cloud Computing". In: *arXiv preprint arXiv:2401.04552* (2024).

[II18] Nigar Ismayilova and Elviz Ismayilov. "Convergence of hpc and ai: two directions of connection". In: *Azerbaijan Journal of High Performance Computing* 1.2 (2018), pp. 179–184.

[Jaj+16] Sushil Jajodia et al. "Cyber deception". In: *Springer* 1 (2016), pp. 2–1.

[Jia+20] Jianxin Jiao et al. "Towards augmenting cyber-physical-human collaborative cognition for human-automation interaction in complex manufacturing and operational environments". In: *International Journal of Production Research* 58.16 (2020), pp. 5089–5111.

[JL23] Jaehoon Paul Jeong and Patrick Lingga. "CBSS: Cloud-Based Security System with Interface to Network Security Functions". In: *2023 Fourteenth International Conference on Mobile Computing and Ubiquitous Network (ICMU)*. IEEE. 2023, pp. 1–8.

[JTS] Lija Jacob, KT Thomas, and M Savithri. "AI in Forensics: A Data Analytics Perspective". In: *Artificial Intelligence for Cyber Defense and Smart Policing*. Chapman and Hall/CRC, pp. 41–60.

[KA23] Harmeet Kaur Khanuja and Aarti Amod Agarkar. "Towards gan challenges and its optimal solutions". In: *Generative Adversarial Networks and Deep Learning*. Chapman and Hall/CRC, 2023, pp. 197–207.

[KTW23] Ivan Kraljevski, Constanze Tschöpe, and Matthias Wolff. "Limits and prospects of big data and small data approaches in ai applications". In: *KI-Kritik/AI Critique Volume 4* (2023), p. 115.

[Lea+23] Deep Learning et al. "ECE49595CV: Computer Vision Fall 2023 Course Information Course number and title: ECE49595CV (003) Computer Vision CRN: 24034". In: (2023).

[LZ24] Tao Li and Quanyan Zhu. "Symbiotic game and foundation models for cyber deception operations in strategic cyber warfare". In: *arXiv preprint arXiv:2403.10570* (2024).

[MK23] Thavaselvi Munusamy and Touraj Khodadi. "Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security". In: *Journal of Informatics and Web Engineering* 2.2 (2023), pp. 59–71.

[MPK23] Vinay Mallikarjunaradhya, Ameya Shastri Pothukuchi, and Lakshmi Vasuda Kota. "An overview of the strategic advantages of AI-powered threat intelligence in the cloud". In: *Journal of Science & Technology* 4.4 (2023), pp. 1–12.

[MS] Ashok Manoharan and Mithun Sarker. "REVOLUTIONIZING CYBERSECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR NEXT-GENERATION THREAT DETECTION". In: ().

[NDT24] Meghna Manoj Nair, Atharva Deshmukh, and Amit Kumar Tyagi. "Artificial intelligence for cyber security: Current trends and future challenges". In: *Automated Secure Computing for Next-Generation Systems* (2024), pp. 83–114.

[NLS23] Philippe Olivier Alexandre Navaux, Arthur Francisco Lorenzon, and Matheus da Silva Serpa. "Challenges in high-performance computing". In: *Journal of the Brazilian Computer Society* 29.1 (2023), pp. 51–62.

[Osm+23] Nahdia Maryam Osmani et al. "Cloud Computing Security Challenges, Threats and Vulnerabilities". In: *Mathematical Statistician and Engineering Applications* 72.1 (2023), pp. 1446–1454.

[Ped24] Hans Pedersen. "EXISTENTIALISM AND ARTIFICIAL INTELLIGENCE IN THE 21ST CENTURY". In: *The Routledge Handbook of Contemporary Existentialism* (2024), p. 36.

[Pei17] Sean Peisert. "Security in high-performance computing environments". In: *Communications of the ACM* 60.9 (2017), pp. 72–80.

[PJ24] Dragan Petrović and Milena Jovanović. "Synergistic Potential of Supercomputing and AI in Shaping Secure Digital Environments". In: *Quarterly Journal of Emerging Technologies and Innovations* 9.1 (2024), pp. 61–76.

[Raw+21] Atul Rawal et al. "Recent advances in trustworthy explainable artificial intelligence: Status, challenges, and perspectives". In: *IEEE Transactions on Artificial Intelligence* 3.6 (2021), pp. 852–866.

[Rob24] RobFarber. *Use cases show that on-package accelerators benefit HPC/AI workloads from computation to data movement and security.* en-US. Mar. 2024. URL: `https://www.datasciencecentral.com/use-cases-show-that-on-package-accelerators-benefit-hpc-ai-workloads-from-computation-to-data-movement-and-security/`.

[SLF23] Muhammad Fakhrul Safitra, Muharman Lubis, and Hanif Fakhrurroja. "Counterattacking cyber threats: A framework for the future of cybersecurity". In: *Sustainability* 15.18 (2023), p. 13369.

[SP10] Robin Sommer and Vern Paxson. "Outside the closed world: On using machine learning for network intrusion detection". In: *2010 IEEE symposium on security and privacy*. IEEE. 2010, pp. 305–316.

[SVF16] Nader Sohrabi Safa, Rossouw Von Solms, and Steven Furnell. "Information security policy compliance model in organizations". In: *computers & security* 56 (2016), pp. 70–82.

[Tha24] Manikant Thakur. "Cyber Security Threats and Countermeasures in Digital Age". In: *Journal of Applied Science and Education (JASE)* (2024), pp. 1–20.

[Tym+23] Miller Tymoteusz et al. "REINFORCEMENT LEARNING: A DRIVING FORCE IN THE EVOLUTION OF SCIENCE AND INFORMATION ACTIVITY". In: *The 13th International scientific and practical conference "Information activity as a component of science development"(April 04–07, 2023) Edmonton, Canada. International Science Group. 2023. 580 p.* 2023, p. 449.

[Veg+24] Christian Vega et al. "Machine learning controller for data rate management in science DMZ networks". In: *Computer Networks* 242 (2024), p. 110237.

[Vel24] Andreja Velimirovic. *How do HPC and AI work together?* en-US. Jan. 2024. URL: `https://phoenixnap.com/blog/hpc-ai`.

[Wu20] Yuming Wu. "Mining threat intelligence from billion-scale SSH brute-force attacks". PhD thesis. University of Illinois at Urbana-Champaign, 2020.

[Yan+19] Qiang Yang et al. "Federated machine learning: Concept and applications". In: *ACM Transactions on Intelligent Systems and Technology (TIST)* 10.2 (2019), pp. 1–19.

[Yan+21] Boxiong Yang et al. "Research on network security protection of application-oriented supercomputing center based on multi-level defense and moderate principle". In: *Journal of Physics: Conference Series*. Vol. 1828. 1. IOP Publishing. 2021, p. 012114.

[Zha+22] Zhibo Zhang et al. "Explainable artificial intelligence applications in cyber security: State-of-the-art in research". In: *IEEE Access* 10 (2022), pp. 93104–93139.