HPS

Michael Hubert Duah

Security in Cloud and HPC

Seminar: Newest Trends in High-Performance Data Analytics

Table of contents

Cybersecurity Landscape

- The use of the Internet in almost every step of today's lifestyle, from the banking system, and business world to all confidential communications has created a lot of vulnerability in our privacy and security. The role of Internet in the government organizations, private companies, social media, military, and financial institutions has made the cyber security issue a national security issue.
- The development of new and innovative cyber defense systems equipped with much more effective algorithms, tools, and protocols is the need of the hour to help protect our cyberspace users.
  Pandey, Tripathi, and Vashist, "A survey of cyber security trends, emerging technologies and threats"

Security Concerns in Cloud and HPC

- Cloud computing is a model for delivering computing resources over the internet. Cloud computing allows users to access computing resources on-demand, without having to invest in expensive hardware or infrastructure. Cloud computing is often used for data storage, application hosting, and other computing tasks that can be performed remotely. Aside from that, it faces several security threats and issues, which may slow down the adoption of cloud computing models.
  Lynn et al., "Understanding the determinants of cloud computing adoption for high performance computing"

High-performance Computing Threats

- High-Performance Computing (HPC) refers to the use of supercomputers and parallel processing techniques to solve complex computational problems that require significant processing power and high-speed computation. HPC systems are designed to deliver performance far beyond that of a typical desktop or server, enabling the processing of large datasets, complex simulations, and advanced scientific and engineering applications. HPC is commonly used in fields such as scientific research, weather forecasting, molecular modeling, financial modeling, and data analytics, where the need for massive computational capabilities is essential.
  Navaux, Lorenzon, and Silva Serpa, "Challenges in high-performance computing"

Cybersecurity Landscape

- In recent years, there has been a growing trend towards using cloud computing for HPC workloads. This has led to the development of specialized cloud services and platforms that are designed to support HPC applications. These platforms provide users with access to high-performance computing resources on demand, making it easier and more cost-effective to perform complex calculations and simulations.
  Guo et al., High-Performance Computing (HPC) Security: Architecture, Threat Analysis, and Security Posture

Cloud-specific Threats

Figure: *Source: Norton*

Identity and Access Management

- Who has access to certain documents
- Where users are allowed to access documents
- Which devices are permitted access

Figure: Source: Richmond Security

Encryption and Data Protection

Protecting sensitive data is crucial in a Cloud environment. Employ the following encryption best practices

- **Data at Rest:** Enable encryption for data at rest in the database. Use strong encryption algorithms and ensure proper key management practices are in place.
- **Data in Transit:** Encrypt data transmitted between client applications and the Cloud system using secure protocols such as HTTPS or SSL/TLS.
- **Backup Encryption:** Encrypt database backups to prevent unauthorized access to sensitive information if backups are compromised.
  Kunduru, "Industry Best Practices on Implementing Oracle Cloud ERP Security"

Shadow IT

Shadow IT is any information technology an employee uses without IT knowledge approval. This includes:

- Peer-to-peer collaboration tools
- Bluetooth-based sharing tools
- Messaging apps
- Personal laptops, phones, or tablets The rapid migration to cloud services has made shadow IT a prevalent issue, exposing organizations to security hazards that an organization’s IT department likely is not aware of.

Data Breach

- A data breach occurs when information is accessed without authorization. As individuals and organizations migrate to the cloud, data breaches are becoming more prevalent.
- The overwhelming amount of data CSPs store for people and businesses makes them a prime target for a data breach. Often performed by experienced cybercriminals in search of private information, this cloud security risk could put medical documents, financial records, and customer information in jeopardy.

Human error

Human errors are unintentional actions or lack of action that can result in a data breach, like:

- Downloading malware from an infected software
- Using weak passwords
- Compromising an IP address
- Sending information to the wrong recipient
- Not updating web-based software

Cybercriminals often prey on internal vulnerabilities to launch their attacks. But in some cases, users may not even know where their personal security efforts fall short. In fact, human error and misuse were both primary causes of 82% of data breaches in 2022

Zero-day Exploit

A zero-day exploit is when hackers discover a software gap or flaw they can use to gain access to users' information or computers.

- Zero-day attacks are inherently stealthy, so it can take months or even years to be uncovered. But in some cases, developers might be able to stop or patch vulnerabilities before too much damage is caused.

Data loss

Cloud-based systems can fall victim to data loss—just like home and office networks. Data loss can happen as a result of a data breach, natural disaster, or a system-wide malfunction. Truly protecting documents means:

- Reviewing the CSP's backup strategy to ensure there are steps in place to guarantee the Cyber Safety of digital assets
- Take the initiative to back up your data yourself, making the complete destruction of your data near impossible

Network Security in an HPC Environment

- **Insider Threats and Credential Compromise:**
  Insider threats, including compromised credentials, pose a significant risk in HPC environments where users often have elevated privileges.
  Unauthorized access by insiders can result in data theft, tampering, or disruption of critical operations.
  Implement least privilege principles, conduct user behavior monitoring, and enforce strong authentication and access controls to mitigate insider threats.

Shared Responsibility Model

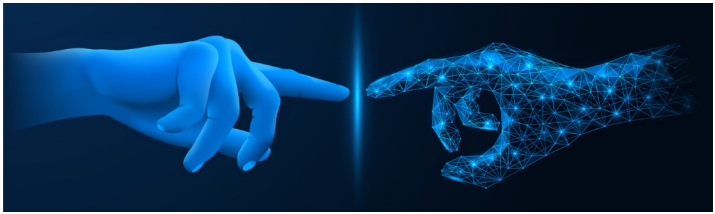

Figure: *source: Sonraisecurity*

- Cloud Service Provider is responsible for hardware and software, including physical data centers, networks, edge locations, and virtualization layers.
- Customers are responsible for securing their own applications and data, and managing access controls and configurations within their accounts

Shared Responsibility Model

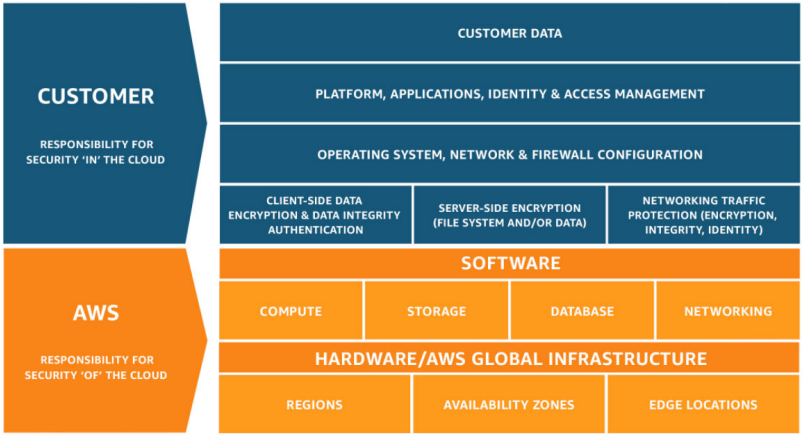

Figure: *2. AWS Shared Responsibility Model*

GCP Shared Responsibility Model

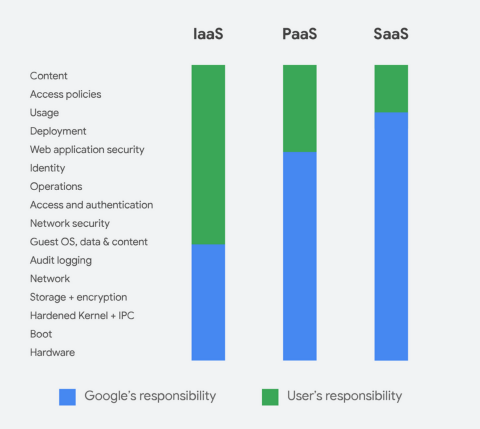

Figure: *Source: Google*

Microsoft Shared Responsibility Model

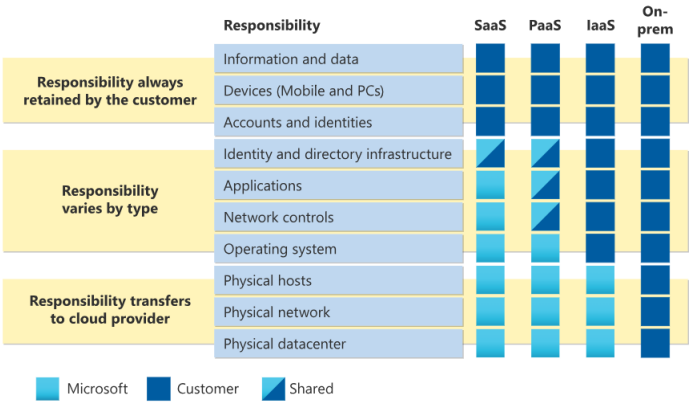

Figure: *Source: Microsoft*

HPC Security Measures

- **Access Control:** Implementing strong access controls, including user authentication, authorization, and role-based access, to restrict system access to authorized personnel only.
- **Network Security:** Deploying firewalls, intrusion detection and prevention systems, and network segmentation to safeguard HPC networks from unauthorized access, malware, and cyber attacks.
- **Incident Response:** Developing and regularly testing incident response plans to effectively respond to security breaches, minimize impact, and restore normal operations.
- **User Training and Awareness:** Providing security training and awareness programs for HPC system users to promote good security practices and mitigate the risk of insider threats.

AI and Machine Learning in Threat Detection

- Adaptive Threat Detection
- Predictive Analytics
- Automation
- Tailored Security Solutions

Figure: Source: Aria cybersecurity

AI and Machine Learning in Threat Detection

- **Adaptive Threat Detection:**
  Adaptive threat detection involves the continuous learning and adjustment of security measures based on evolving threats.
  Advanced machine learning algorithms adapt to new attack patterns in real-time, enhancing the system's ability to identify and respond to emerging threats.
  Improved detection accuracy, reduced false positives, and enhanced resilience against previously unseen threats.

AI and Machine Learning in Threat Detection

- **Predictive Analytics:**
  Predictive analytics leverages historical data and machine learning models to forecast potential future security threats.
  Machine learning algorithms analyze patterns, behaviors, and anomalies to predict potential security incidents before they occur.
  Proactive threat mitigation, quicker response times, and improved overall cybersecurity posture.

AI and Machine Learning in Threat Detection

- **Automation:**
  Automation involves the use of AI and machine learning to perform security tasks without human intervention.
  Technology Implication: Automated threat detection and response systems can analyze vast amounts of data, identify threats, and initiate responses at machine speed.
  Benefits: Reduced response time, increased efficiency, and the ability to handle large-scale security incidents.

AI and Machine Learning in Threat Detection

- **Tailored Security Solutions:**
  Tailored security solutions involve the customization of AI and machine learning models to specific organizational needs and threat landscapes. Machine learning models are fine-tuned based on the unique characteristics and requirements of an organization, optimizing threat detection capabilities.
  Improved accuracy by considering context-specific factors, better alignment with organizational objectives, and adaptability to changing threat landscapes.

Quantum Computing Implications

- **Secure Communication:** Quantum computing offers the potential for secure communication through quantum key distribution (QKD) protocols, which leverage the principles of quantum mechanics to enable the exchange of encryption keys with unconditional security. This could lead to the development of highly secure communication networks resistant to eavesdropping and interception.
- **Cybersecurity:** Quantum computing may also contribute to advancements in cybersecurity by enabling more robust and efficient methods for threat detection, anomaly detection, and secure data transmission, thereby enhancing overall cybersecurity posture.
  Navaux, Lorenzon, and Silva Serpa, "Challenges in high-performance computing"

Summary

In the ever-evolving world of cybersecurity, staying ahead of threats is not just a matter of strategy but of survival. As we look to the future, several emerging trends and technological advancements are set to redefine the landscape of Security in Cloud Computing and HPC.

Organizations must stay abreast of these trends, adapt their strategies accordingly, and navigate the associated challenges responsibly. The journey ahead for cyber threat intelligence is as exciting as it is crucial in shaping a resilient cybersecurity landscape

Conclusion

We look to the future for transformative changes, with AI and ML leading the charge. As these technologies evolve, they will enable more sophisticated, efficient, and proactive approaches to security in Cloud and HPC. However, the human element will remain indispensable, and collaborative efforts across industries and borders will be key to creating a more secure digital world.

References

Guo, Yang et al. *High-Performance Computing (HPC) Security: Architecture, Threat Analysis, and Security Posture*. Tech. rep. National Institute of Standards and Technology, 2023.

Kunduru, Arjun Reddy. “Industry Best Practices on Implementing Oracle Cloud ERP Security”. In: *International Journal of Computer Trends and Technology* 71.6 (), pp. 1–8.

Lynn, Theo et al. “Understanding the determinants of cloud computing adoption for high performance computing”. In: *51st Hawaii International Conference on System Sciences (HICSS-51)*. University of Hawai’i at Manoa. 2018, pp. 3894–3903.

Navaux, Philippe Olivier Alexandre, 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.

Pandey, Anand Bhushan, Ashish Tripathi, and Prem Chand Vashist. “A survey of cyber security trends, emerging technologies and threats”. In: *Cyber Security in Intelligent Computing and Communications* (2022), pp. 19–33.