Research on Network Security Protection of Application-Oriented Supercomputing Center Based on Multi-Level Defense and Moderate Principle

Boxiong Yang1,2, Ying Yu1,2,*, Zeyu Wang1,2, Shelei Li1,2, Huling Gao1,2, Zhiyong Liang1,2, Xue Zhou1,2

1 School of Information & Intelligence Engineering, University of Sanya, No. 191, Xueyuan Road, Sanya City, Hainan Province, China
2 Academician Workstation of Chunming Rong, University of Sanya, No. 191, Xueyuan Road, Sanya City, Hainan Province, China
*Email: 569434537@qq.com

Abstract. High Performance Computing (HPC), also known as Supercomputing, is widely applied in various fields, which have the advantage of high processing capability and mass storage. Various open business services bring great threat to the network and data security of HPC cluster. This paper proposes a feasible scheme to realize supercomputing information security through multi-layer defense and overheads control according to the experience of operation, management and maintenance of Supercomputer Center for many years. First, this paper puts forward the principle of moderate risk, and gives the principles of design and the implementation for the security protection of Supercomputing Center. Second, this paper presents a security system architecture in coordination with deep collaborative defense. Finally, this paper designs a 4-layer protection scheme on account of the latest network security solutions and the operation and maintenance characteristic of our own supercomputer. Experiments on multi-level defense and overheads control show that the designed scheme takes into account the cost and network security, and obtain prospective results, which is especially suitable for the network security protection of small-scale or medium-scale high-performance computing cluster for engineering application.

1. Introduction

In recent years, with the rapid development of big data, cloud computing, Artificial Intelligence and other technologies, the application scope of supercomputing is expanding continuously. Cluster computing has been widely used to improve computing capabilities and plays an important role in many application fields. Supercomputing has become an important index to measure a country's scientific and technological capability [1-5]. Nowadays, a variety of high-performance supercomputing centers have been established with the need of economic development. Supercomputing technology has gradually developed from scientific research to industrial application. Therefore, security, reliability and scalability have become the most important issues in supercomputing applications [6-9].

At present, the security situation of computing cluster and storage unit in Supercomputing Center is not optimistical. The supercomputing cluster is forced to invest as much computing power as possible into scientific computing because the scale of the problem to be solved is more and more large and the...
accuracy is higher and higher, which makes many security protection technologies difficult to be applied on a large scale due to the consumption of more computing resources, which further worsens the security situation of supercomputing clusters and storage units [10-13].

In summary, these security risks mainly exist in the following aspects:

1) Operating system security vulnerabilities

Even if the open-source Linux operating system also has security vulnerabilities, the intruder can use the security vulnerability to enhance their own rights, steal important data or destroy the normal software environment, resulting in data loss or service stop of the whole cluster system [14-17].

2) Malware attack

It is impossible to identify and prevent the attacks caused by malicious programs written and executed by intruders under the existing independent access control (DAC) mechanism of Linux, such as Trojan horse, privilege operation and malicious consumption of computing resources. The reason is that it is allowed to compile, transplant and run the required computing software in the cluster system [1-20].

3) Internal network security risk

Supercomputing cluster is a distributed system composed of independent computer nodes and high-speed networks. In order to ensure the smooth operation and performance maximization of large-scale parallel computing programs such as MPI, the security software inside the nodes is closed, and the mutual trust access control mechanism is used between nodes, resulting in the intrusion behavior of single node can be easily copied and spread to the whole cluster system [21-25].

From the above analysis, we can see that supercomputing cluster should consider both internal and external security protection. Because of its pursuit of performance maximization, it is necessary to choose the technical means with less resource consumption. In addition, we also need to develop a certain security management strategy to make up for the lack of technical means. On the other hand, Application-Oriented Supercomputing Center will become a direction of supercomputing development in the future from the long-term development of supercomputing while the management cost and maintenance cost will become the bottleneck problem restricting the development of supercomputing [26-30].

2. Design Principles

Hierarchical protection is an important strategy for building the firewall of network information security [31], the key of which is to construct, manage and supervise the information system according to different levels and standards. As for the supercomputing center system with high investment, strong security and emphasis on application, we should take “moderate risk” as the core, proceed from the business point of view, and take key protection as the principle, that is to focus on the protection of important business information systems. In the scheme design, the following principles should be followed.

2.1. Principle of Moderate Safety

As is known to all, any computer information system is impossible to achieve absolute security. In the process of constructing the network information security system of the supercomputing center, security requirements, security risks and security costs should be balanced and compromised. Excessive security requirements will increase costs and operational complexity, which will be counterproductive and reduce the efficiency of the system.

Moderate security is the original intention of hierarchical protection. On the one hand, strictly following the basic requirements, protection measures should be strengthened in terms of networks, hosts, applications, and data to ensure the confidentiality, integrity and availability of information systems during the construction of supercomputing. On the other hand, the corresponding protection intensity is proposed for the actual risk in the operation and maintenance process of the supercomputing system, and the safety protection system is designed and constructed according to the protection intensity, so as to effectively control the cost.
2.2. **Principle of Critical Protection**
The information systems with different security protection levels are divided into different security protection intensities according to the importance and business characteristics of supercomputing system, and the information systems including core business or key information assets are centralized protected Preferentially.

2.3. **Principle of Equal Emphasis on Technical Management**
The problem of information security is not a simple technical problem. Information security has a certain preventive effect on hacker invasion or virus intrusion, but it is difficult to solve all information security problems by system security deployment. Combine technical measures with management measures to ensure the Intranet Information System security of the whole Supercomputing Center more effectively, so as to form the effective integration of technology and management.

2.4. **Principle of Standardization**
The information security protection system of supercomputing center should comply with the international, national and local security standards, such as ISO 27001, GB/T 22239-2008, so as to make the hierarchical protection system more extensive after completion of the supercomputing system.

2.5. **Principle of Dynamism**
Information security issues are not always static, but change with the changes of organizational structure, organizational strategy and information system operation procedures related to the management of supercomputing center. Therefore, it is necessary to track the changes in the information system to adjust security protection measures.

2.6. **Principle of Maturity**
The security measures in the construction of the supercomputing center should be mature in technology could be tested to solve the security problems and have been successfully applied in many projects.

3. **Design Scheme**

3.1. **Intelligence Clues Instead of Technical Confrontation**
Traditional means of security defense are often based on attack-defense technical confrontation, which can effectively counter the standard attack behaviors on the premise of obtaining the details of the attack, but powerless to attacks with complex camouflage and bypass means. The attack-defense technical confrontation is just like a contradiction between spears and shields. In reality, there is always spear before shield. Therefore, the traditional confrontation ideas cannot deal with unknown threats. Typical examples, such as unknown Trojans and unknown vulnerabilities, are the most difficult in traditional security defense.

New defense technologies emphasize the threat in the value and use of threat intelligence. Threat intelligence no longer relies solely on attack-defense technical confrontation, but rather finds valuable suspicious clues in the entire network activity, and further explores a series of behavioral activities behind these clues combined with the existing massive historical data. In this way, will be a complicated APT attack detection is decomposed into a simple clue discovery and information mining, which is not only solves the problem that APT and other complex attacks cannot be detected, but also circumvents the problem that technology alone is difficult to confront, and at the same time achieves "offensive and defensive inversion". Relying on the idea of technical confrontation in the past, as long as the defensive side failed a confrontation, the attacker would successfully infiltrate. It only takes one wrong move to end in a total defeat. But now, relying on the idea of threat intelligence clues, as long
as the clue is caught once, the defender could use this clue to capture the attack. Throughout the defense process, 1% success for the attacker means 100% success. The "offensive and defensive inversion" changes the previous unequal contest between the two sides completely.

3.2. Space for Time Instead of Single-point Detection
In the new defense technology, the value and use of threat intelligence are emphasized the key point of the new defense system is to exchange the detection time through data space. The essence between offense and defense is a chase game. If the attacker is discovered and intercepted before launching an effective attack, the attack information, called threat information, will be recorded, which has high security value. Through threat intelligence, the security system may be able to prevent in advance. Even before the attacker launches the attack, the defense system has been prepared to prevent illusion. For example, some hacker organizations, such as Anonymous, often discuss the target and method of attack on a forum a few days before launching an attack. If you can obtain this information in advance, you can conduct targeted monitoring and defense against these attacks.

3.3. Data Centric Instead of Technology Centric
"Data Driven Security" is the core of the new security system. Data is the most essential content of the new security system. The core content, specifically rely on a wide range of data analysis to achieve the perceived threat, discovery, analysis, traceability, and emphasizes the use of traditional security defense system attack-defense technology in a segment of the attacks found attacks, by contrast, this line of thinking more confined to the traditional security defense system at a certain moment to attack behavior found that like to attack at a particular moment of photograph, is static, local, cannot have a comprehensive understanding about the outline of the attack, And once the attack fragment is missed, the attack cannot be found again.

The new defense technology takes data as the core, which is equivalent to recording the whole attack process, and then performing a retrospective analysis of the entire attack process. It can not only understand the full picture of the attack, but also be possible to capture the attack at any link or fragment in the whole process of the attack. In addition, taking data as the core is essentially a kind of "security crowdfunding" system, that is, once an unknown attacker enter into the data system, the data system will realize detection and defense capabilities and position this attack. This is impossible to achieve in a traditional technology-centric security system.

3.4. Multi-dimensional Collaborative Operations
The protection capabilities of information system need to be improved from multiple dimensions, which not only relies on localized security equipment, but also needs require dynamic security intelligence.

A new cognition must be established: if there's a discovery, there's protection, and if there is protection, there will be risks. Based on the new security cognition, it is necessary to expand the concept of protection, establish a multi-dimensional local protection system, combine with cloud security and big data to generate threat intelligence, and finally form targeted intelligence and other ecological protection, as shown in Figure 1.
Figure 1. Multi-Dimensional Ecological Protection System.

- **Early warning ability**
  Utilizing cloud threat intelligence, Internet security public measurement and situational awareness capabilities, the information system is given the capability of early warning, which can accurately determine the attack behavior from the massive security data, and protect the information system in advance.

- **Protection ability**
  The security technology and control measures of hierarchical protection will be replaced and enhanced by new technology products. Meanwhile, the overall information system protection capability is improved by combining with the cloud protection capability.

- **Traceability**
  Integrate threat intelligence and local full data, through visual analysis technology, can quickly locate security risks, and then form an intelligent security management center.

4. **Security Protection System**

4.1. **Defense-In-Depth System**
Responding to the threats caused by changes in internal infrastructure, a hierarchical, centralized, and differentiated protection system should be set up. Establish multi-layer security and security measures in depth from network layer security, host security, application layer security and operation security to ensure the security of user information and information system. In the strategy of defense in depth, human, technology and operation are the three main core factors. To ensure the security of information and information system, all three are indispensable.

4.2. **Collaborative Defense System**
In order to deal with the threats caused by the scale change of external attacks, the attack should be dealt with first outside the information system, and self-built or distributed protection by security service providers can be used. Through our many years of operation experience, it is difficult to guarantee the safe operation of information system under specific conditions such as large-scale denial of service attack, variant attacks and new malicious code attacks only relying on our own security protection system. Therefore, it is necessary to cooperate with other security manufacturers to establish a collaborative protection system combining big data technology and professional security protection capabilities.

5. **Solutions**
Taking the network security construction of the Supercomputing Center of University of Sanya as an example, based on the security requirements analysis and design ideas mentioned above, it focuses on network security, host security, application security and operational security. The information security system of the supercomputing center is constructed with the four levels of improving the system's ability of perception, detection, protection and response. The security protection system architecture of the entire supercomputing center is shown in Figure 2, which is divided into four layers.

**Figure 2.** Security Protection Architecture of Supercomputing Center.

5.1. 1-Level
Deploy the next generation firewall at each security boundary, enable intrusion prevention and anti-virus function to achieve access control on the flow, intrusion attack defense and malicious code prevention of the passing traffic. Moreover, it can combine external threat intelligence, terminal security management system and unknown threat perception system to generate dynamic rules and form automatic defense.

5.2. 2-Level
Deploy an operation and maintenance audit system in the field of security management to achieve multi-functional management based on account management, identity authentication, resource authorization, access control, operation and maintenance audit for the operation and maintenance personnel.

5.3. 3-Level
The deployment of a terminal security management system and a set of network security access system, which cooperate with quota sum to realize multiple security management functions such as malicious code detection and prevention, vulnerability patch repair, security operation and maintenance management, security baseline access for terminals and servers of the whole network. It will link unknown threat perception system with next generation firewall to realize dynamic defense.
5.4. 4-Level
The deployment of an unknown threat awareness system consists of two components: a traffic acquisition probe and analysis platform. A traffic acquisition probe is deployed in the bypass of the Intranet network core switch to collect the mirror traffic of the core switch, and then the traffic is restored and uploaded to the analysis platform. At the same time, in the process of collecting traffic, a variety of detection engines built into the probe will identify the attack behavior mixed in the traffic, and the detection results will be summarized into the analysis platform. The analysis Platform has built in large data analysis engine, which combined with the external threat intelligence local collision, mass data storage, intelligent analysis, modelling, machine learning and can recognize unknown attacks. At the same time, based on the correlation analysis technology, it can trace the source of the attack, replay the attack process, and link the firewall and terminal security management system to achieve intelligent blocking of unknown threats.

6. Implementation Effects

6.1. Network Isolation and Access Control
By deploying next-generation firewall devices at each important network security boundary, realize the logic series isolation between internal and external networks can be achieved, while logical isolation between different internal security zones can be achieved to effectively control network access. First, it can achieve one-way access requirements between networks and filter some unsafe services; second, it can achieve secure access control based on conditions such as protocol, port number, time, and traffic, with a strong logging function; finally, It can record all the access behaviors of disturbed meetings based on the strategies required by different communication networks, and can intelligently link with threat intelligence to form an integrated protection system of cloud perception and boundary control. The implementation effect of network isolation and access control is shown in Table 1.

| Index                        | Implementation Effects                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Integrated Security Defense  | It supports integrated access control, user-authorized access, intrusion prevention, virus prevention, application layer comprehensive security protection, etc., and cover the IPv4 network and IPv6 network security filtering.                                                                                                                                                                                                                                                                                                             |
| Status Security Filter       | Support for basic, extended and interface-based state detection packet filtering technology. Support for application-level packet filtering protocols. Supports maintenance monitoring of each connection status information and dynamic packet filtering, support the application layer protocol status monitoring.                                                                                                                                                                                                                     |
| Access Control Features      | Supports access control based on source IP, destination IP, source port, destination port, time, service, user, MAC address, and other methods. Supports traffic management, connection number control, IP+MAC binding, user authentication, etc.                                                                                                                                                                                                                                                                                                                                 |
| Support for NAT Application  | Support multi-to-1, multi-to-many, static network segment, bidirectional conversion, IP and DNS mapping and other NAT applications; support multiple application protocols to traverse NAT correctly                                                                                                                                                                                                                                                                                                                                 |
| Defense for Three-Dimensional Cooperative | It can achieve intelligent linkage with threat intelligence, virus cloud detection, Trojan cloud detection, etc., to build a "cloud + border + linkage" new generation security defense system for the Supercomputing Center.                                                                                                                                                                                                                                                                                                      |

6.2. Network Intrusion and Virus Defense
The ability to turn on intrusion prevention in firewalls, to identify intrusions occurring in the network in a timely manner and make real-time blocking, to defend against new types of hybrid attacks, to monitor and analyse events occurring in computer systems and networks, and to look for intrusions that compromise the confidentiality, integrity, availability or trying to bypass the security mechanisms, of intrusion defense is automatically perform the monitoring and analysis process, and can make effective security guarantees such as effective warning and blocking. The implementation effect of network intrusion and virus defense is shown in Table 2.

Table 2. Network Security Effect.

| Index                        | Implementation Effects                                                                 |
|------------------------------|----------------------------------------------------------------------------------------|
| Vulnerability Protection     | Support the vulnerability protection function and classifies the vulnerability protection feature library, including buffer overflow, cross-site scripting, denial of service, malicious scanning, SQL injection, WEB attacks, etc. Supports application protocol-based vulnerability protection. |
| High-Risk Attack Identification | It can attack characteristics high-risk vulnerabilities such as "Eternal Blue", "Stuxnet III", "Dark Cloud III", "Struts", "Struts2", "XShell backdoor code" and other attacks. It also identifies the name, CVEID, CNNVDID, severity, affected platform, type, description, and other details of the corresponding attack. It can filter all kinds of network viruses in the network exchange data, can defend against viruses, Trojan horses, worms, and support for compressed data, casing virus detection and killing, while a variety of broad viruses for comprehensive interception, to prevent the rapid spread of viruses through the network, and will spread through the network virus blocked out. |
| Comprehensive Virus Protection | For HTTP/FTP/POP3 / SMTP, IMAP/SMB virus killing six kinds of protocols. It also supports decompression of compressed files of up to 6 levels, as well as MD5-based custom virus signatures. |
| Centralized Access Control   | The centralized and unified access control and granular command-level authorization policy, while ensuring the minimum privileges required for users to complete tasks, and centralized and orderly operation management to prevent illegal and unauthorized access incidents. |
| Centralized Security Audit   | Based on unique identification, by auditing the user's entire operation behavior from login to exit, monitoring the user to all sensitive and critical operations in the managed devices, providing graded alarms, focusing on the critical time, to achieve timely early warning of security events and accurate detection and investigation. |

6.3. Server Security Reinforcement

Deploy a server security management system for key application servers to provide security reinforcement, threat perception, risk discovery, intrusion detection, event backtracking, automation all-around security protection capability. In order to help the Supercomputing Center of University of Sanya to discover and defend against hacking activities against key application servers, such as CC attacks, SQL injection, XSS cross-site, vulnerability exploitation, Trojan horses, backdoors. The server security management system uses big data technology to analyse the attack monitoring data globally. After installation, it can effectively perceive and evaluate the overall security status of key application information systems. The implementation effect of server security reinforcement after implementation is shown in Table 3.
### Table 3. Implementation Effect of Server Security Reinforcement.

| Index                  | Implementation Effects                                                                                                                                                                                                                                                                                                                                 |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advanced Protection    | Intercept Web Shell and discover vulnerabilities in Web programs in time to protect against attacks that exploit the vulnerabilities, which contains known Web Shell auto-isolation, unknown Web Shell real-time protection, SQL injection vulnerability protection, file upload vulnerability protection, Struts2 vulnerability protection, deserialization vulnerability protection, arbitrary file read-write, vulnerability protection, command execution vulnerability, and so on. |
| Backtracking of Attacks | The system will generate corresponding security logs in the three stages of risk identification, defense and threat awareness. Server reinforcement systems will be automatically associated and event analysis reports will be generated. For intrusion-type attack events, the system will automatically backtrack the attack process, quickly locates and repairs the risk points. |
| Rational Control of Resources | The system provides three monitoring functions: real-time monitoring, system resource monitoring and website performance monitoring. By setting alarm threshold, the resource usage can be monitored in real-time. The real-time monitoring, can monitor batch of servers, you can choose the server network, memory or CPU to monitor. System resource monitoring includes CPU usage, memory usage, disk usage, and network IO. Site performance monitoring includes the concurrences of the site, the PV value of the day, requests per second, daily network traffic statistics, and so on. |
| Operating System Reinforcement | Perform a comprehensive and efficient baseline check of host security configuration, including system weak passwords, cloned accounts, and scheduled tasks, etc. Prohibit useless services in the operating system, improve system security, and reduce system resource usage. Through the kernel probe, the operating system can be strengthened, the security and anti-attack ability of the system itself can be improved, and the core files of the system such as file tampering prevention, prohibition of malicious code execution, prohibition of loading drivers without digital signatures can be protected. |

#### 6.4. Security Operations and Maintenance Audit

The network equipment is great in number in the Supercomputing Center, the possibility of human incorrect operation occurs from time to time, and the hacker/malicious access may gain system permission and break into the internal network of the unit, resulting in incalculable losses. Through the deployment of a set of operation and maintenance audit system in the security management area, the centralized management is realized by using the operation agent mode, the identity, access, authority and audit are managed effectively, the operation and maintenance management level of the system is improved, the relevant security policy standards are met, the intrusion and malicious access are prevented, the users’ behaviors on the server is tracked, the operation and maintenance cost is reduced, the control and audit basis are provided, and the operation risk is minimized. The effect of the implementation of the security operation and maintenance audit is shown in Table 4.

### Table 4. Effect of Security Operations Audit.

| Index                   | Implementation Effects                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Centralized Account Management | Global real name system management based on unique identity supports unified account management strategy, realizes seamless connection with each server, network equipment and so on, and centrally manages the main account (ordinary user), slave account (target equipment system account) and related attributes. |
Centralized Access Control Through centralized and unified access control and fine-grained command-level authorization policy, we can ensure the minimum permissions required by users to complete the task, realize centralized and orderly operation and maintenance operation management is realized to prevent illegal and unauthorized access events.

Centralized Security Audits Based on unique identity identification, it monitors all sensitive and critical operations of users on managed devices through auditing the entire operation behavior of users from login to launch, provides hierarchical alarm, focuses on critical time, and realizes timely early warning discovery and accurate checking of security incidents.

7. Conclusion
After a comprehensive analysis of the various network threats, attacks and hidden security risks often suffered by applications in supercomputing center, this paper makes a further study of the security protection methods used in current supercomputing systems. On this basis, the principle of "moderate risk" in the supercomputing network security scheme is put forward in this paper, and some design ideas are proposed, which are suitable for setting up and protecting the network security of application-oriented supercomputing center.

According to the principle of "moderate risk" proposed in this paper, the supercomputing scheme has been proved to be effective. The system has been operating for more than a year. Although it has been attacked by many parties, our system is in good condition. It achieves a balance between cost and security level. The security risk of supercomputing can be controlled to ensure the virtuous cycle of supercomputing application and the controllable risk of investment income. The research in this paper can provide reference and reference for the security protection in the construction process of small and medium-sized supercomputing (cluster peak computing scale is one hundred trillion TFLOPS), make the supercomputing system meet the security requirements of grade protection, improve the security protection capability of the system, and lay a solid foundation for the operation, management and maintenance of the supercomputing system. The measures adopted can be changed with the change of information system security requirements, with extensibility and upgradability, in order to adapt to the development and expansion of the supercomputing system, on the one hand to avoid repeated investment and construction and economic losses caused by information security incidents. At the same time, it can also avoid the disruption of business information security and system service security, resulting in serious damage to social order and public interests.

Acknowledgements
We would like to thank all the anonymous reviewers for their insightful comments. We also thank Kainan Liu, Tao Yang, Bo Zhou, Ming Yang for reviewing the paper before submission. Meanwhile, we thank Sugon Company very much for technology support. This paper is supported by the Natural Science Foundation of Hainan Province (No. 2019RC257) and Hainan Provincial Department of Science and Technology (No. Hnky2019-69).

References
[1] Hou, T, Wang, T, Shen, D, Lu, Z, and Liu, Y 2020 Autonomous security mechanisms for high-performance computing systems: review and analysis. *Adaptive Autonomous Secure Cyber Systems* 2 109-29
[2] Smari W W, Spalazzi L, and Zemali Y. 2013 Editorial: Recent Developments in High Performance Computing and Security: An Editorial (Elsevier Science Publishers) pp 3-7
[3] Rao N S V, Imam N, Ma C Y T, et al. 2019 Defense Strategies and Expected Capacity of High-Performance Computing Infrastructures 20th International Conference on Distributed Computing and Networking 1 143-7
[4] LI Jun D W 2018 Overview of High-Performance Computing Applications (Beijing, China: Tsinghua University Press) 6 214-31
[5] Zhu G H, Zeng Y H, and Guo M 2017 A security analysis method for supercomputing users’ behavior. CSCloud 2017 287-93.

[6] Ning Z, Bing W, Gang D 2013 Application and development of guangzhou supercomputing center Computer Engineering and Science 11 187-90

[7] Smari W W, Spalazzi L, Zemali Y 2013 Recent developments in high performance computing and security: an editorial Future Generation Computer Systems 29(3) 782-7

[8] Kim J H and Ryu J K 2013 Recent trends on high-performance computing and security Cluster Computing 16(2) 207-8

[9] Tie N, Peng Z, Zongyan C, et al. 2011 Security measures for supercomputing cluster e-Science Technology and Application 2 45-51

[10] Ali M, Khan S U, and Vasilakos A V 2015 Security in cloud computing: opportunities and challenges Information Sciences 305 357-83

[11] Liu D, Zhao Y, Xu H, et al. 2015 Opprentice: towards practical and automatic anomaly detection through machine learning Internet Measurement Conference. ACM pp 211-224

[12] McMahon P and Hutchison A. 2013 A security architecture for high performance computing facilities Computer Physics Communications 97 16-35

[13] Hu H, Zhao Y, Niu T, and Cao R Q 2018 Summary of monitoring platforms for clusters. e-Science Technology and Application 47(01) 81-90

[14] Peisert S 2017 Security in high-performance computing environments Communications of the ACM 60(9) 72-80

[15] Taufer M, Mohr B, and Kunkel J M 2016 High performance computing providing security in container-based HPC runtime environments 10 685-95

[16] Spalazzi L and Vigano L 2015 Special issue on security and high-performance computing systems. Journal of Computer Security 23(5) 539-40

[17] Kim T H, Rana O F, Tourino J, et al. 2011 Special issue on Theory and practice of high-performance computing, communications, and security Journal of Supercomputing 55(2) 123-5

[18] Gong L, Wang C, Zhang C, et al. 2019 High-Performance Computing based Fully Parallel Security-Constrained Unit Commitment with Dispatchable Transmission Network IEEE Transactions on Power Systems 34(2) 931-41

[19] Singh A K 2020 High Performance Computing (HPC) Data Center for Information as a Service (IaaS) Security Checklist: Cloud Data Governance Webology 2(16) 14

[20] Sasikumar D, Saravanan Kumar S, and Saravananan T 2018 Analysis of Security Issues and Safety Measurements in High Performance Cloud Computing Systems Journal of Advanced Research in Dynamical and Control Systems 10(14) 1688-93

[21] Nazir M, Kumar D, Ali L, et al. 2018 Critical analysis of high-performance computing (HPC) International Journal of Computer Science and Information Security 16(9) 153-63

[22] Qiang W 2019 Performance and security in cloud computing Journal of Supercomputing 75(1) 1-3

[23] Monti H M, Butt A R, Vazhkudai S 2011 Timely result-data offloading for improved HPC center scratch provisioning and serviceability IEEE Transactions on Parallel and Distributed Systems 22(8) 1307-22

[24] Sangdo L and Jun-Ho H 2018 An effective security measures for nuclear power plant using big data analysis approach Journal of Supercomputing 2018 1-28

[25] Nengzhi J, Tao W, Wenting A N, et al. 2019 Research on SSH secure remote login of Linux high performance computing cluster Modern Information Technology 3(13) 177-9

[26] Kim J H, Ryu J K, et al. 2013 Recent trends on high-performance computing and security Cluster Computing 5 207-8

[27] Peisert S. 2017 Security in high-performance computing environments. Communications of the ACM, 60(9) 72-80

[28] Rosso A D, Min L, and Jing C Y 2014 High Performance computation tools for real-time security assessment 2014 IEEE Power and Energy Society General Meeting 7 27-31
[29] Czarnul P, Proficz J, Drypczewski K 2020 Survey of methodologies, approaches, and challenges in parallel programming using high-performance computing systems Scientific Programming 2020(5) 1-19

[30] Rao N S V, Imam N, Y T Ma C Y T, Seng H, and He F 2019 Defense strategies and expected capacity of high performance computing infrastructures 20th International Conference on Distributed Computing and Networking 1 143–7

[31] Cornelius H 2017 The future of high-performance computing (HPC). Encyclopaedia of Information Science and Technology 6 15-9