THE SECURED SERVER MANAGEMENT FOR BIG DATA ENVIRONMENTS USING HIGH PERFORMANCE COMPUTING BASED OPTIMIZATION MODEL

M. Abishek and A. Jeyapriya
Department of Computer Science, Alagappa University, India

Abstract

Big data environments require secure server management to ensure the safety of sensitive information. The security of servers must be managed to protect data from unauthorized access, tampering, theft, or misuse. Organizations must ensure that their server management system is up to date and implements the latest security technologies to protect against cyber threats. First, organizations must ensure that access to the server is strictly controlled. Access should be granted only to authorized personnel, and all personnel must use secure authentication methods such as multi-factor authentication to access the server. Additionally, access to the server should be monitored to detect any suspicious activities. Organizations should also implement a comprehensive system of security measures to protect the server from malicious attacks. These measures may include firewalls, intrusion detection systems, and antivirus software. Organizations should also ensure that their server is regularly backed up in case of a system failure. This can be done using cloud storage or physical backups stored in a secure location.

Keywords:

Big Data, Sensitive Information, Organization, Cyber Threats

1. INTRODUCTION

Big data environments are evolving more rapidly than ever before. With the increase in data volumes, it is important to secure server management for these environments. Server management is the process of monitoring, controlling, and optimizing the performance of servers and related services. It is essential for big data environments to have secure server management to ensure the safety, security, and reliability of the data [1].

Secure server management is important for big data environments as it ensures the integrity and availability of data. It also helps to protect against unauthorized access, malicious attacks, and accidental data loss or corruption. By regularly monitoring the performance of the server, administrators can respond quickly to any issues that may arise and take the necessary steps to protect the data. Secure server management also helps to ensure the reliability of data and applications [2].

Regular monitoring of the server can identify any potential issues and help administrators to troubleshoot and resolve them quickly. This helps to ensure that applications run smoothly and data remains secure. The secure server management helps to ensure compliance with data protection regulations and other policies [3].

By regularly monitoring the server and ensuring that data remains secure, administrators can help to ensure that their organization is compliant. This can help to prevent costly fines and other penalties that may arise from non-compliance. The secure server management is essential for big data environments. It helps to ensure the safety, security, and reliability of data and applications, as well as helping to ensure compliance with data protection regulations [4].

By regularly monitoring the server and responding quickly to any potential issues, administrators can ensure that their organization's data remains secure and protected [5].

The recent explosion of big data has necessitated the development of new technologies to secure and manage server environments. Secured server management for big data environments is a relatively new innovation that provides enhanced security while allowing organizations to store and access large volumes of data. Secured server management for big data environments is designed to reduce the risks associated with big data while providing administrators with greater control over access and use [6].

It is typically implemented by a combination of advanced authentication methods and encryption. Advanced authentication methods allow administrators to verify user identities and limit access to data based on credentials. Encryption is used to protect stored data from unauthorized access. The use of secured server management for big data environments also provides organizations with the ability to monitor data use and protect against malicious activity [7].

Administrators can configure rules for access and use that can prevent unauthorized users from accessing the system. Additionally, administrators can detect suspicious patterns of usage and take steps to prevent malicious activity from occurring. Secured server management for big data environments also allows organizations to improve their overall security posture [8]. It provides greater control over who can access the system and what activities can be performed. It also allows administrators to track user activity, detect unauthorized changes, and respond quickly to security incidents [9].

The secured server management for big data environments is an important innovation that provides organizations with the ability to store and access large volumes of data while reducing the risks associated with big data. It provides administrators with greater control over access and use, improved security posture, and the ability to detect malicious activity. This innovation is an essential component of any modern organization's data security strategy [10].

2. RELATED WORKS

Big data environments are highly complex systems that require secure server management. Without secure server management, organizations are at risk of data breaches, unauthorized access, and malicious attacks. The issues that must be addressed when it comes to secure server management for big data environments are multifaceted and ever-evolving. One of the biggest issues is the ability to ensure data security and privacy. This involves not just protecting the data itself, but also the systems, networks, and applications that access the data. This

requires the implementation of sophisticated security measures, including encryption, authentication, and access control [11].

Additionally, organizations must be able to detect and respond to any security threats quickly and effectively. Another issue is ensuring the scalability of the systems. As data volumes increase, organizations must be able to scale their systems to accommodate the additional data. This means ensuring that the hardware and software can handle the increased workloads, as well as the data storage and retrieval needs. The organizations must be able to manage the data in an efficient manner [12].

This includes having the proper tools and procedures in place for data quality management, data governance, and data analytics. This ensures that the data is accurate, up-to-date, and compliant with any regulatory requirements. Secure server management for big data environments is a complex and ongoing process that requires ongoing monitoring and attention. Organizations must be able to identify and address potential issues quickly and effectively to ensure the safety and security of their data and systems. By doing so, they can ensure their data is secure, their systems are scalable, and their data is managed in an efficient and compliant manner. Secure server management for big data environments is a major challenge that organizations face today.

It requires a detailed understanding of the data, the associated security risks, and the infrastructure necessary to store and protect the data. With the increasing volume of data produced and stored, organizations must ensure that the data is accessible and secure. One of the biggest challenges with secure server management for big data environments is the sheer size of the data. Big data can easily overwhelm existing security tools and processes. It is essential to have an effective security strategy in place to protect the data from unauthorized access and manipulation. Organizations must deploy robust security tools and policies to ensure data integrity and confidentiality.

Another challenge is the complexity of the infrastructure. Big data environments often require a mix of different types of systems, from cloud-based systems to on-premises servers. Each system must be managed and monitored for security vulnerabilities. Organizations must also ensure that their systems are properly integrated and configured so that data is protected across all systems. Finally, organizations must ensure that their security policies are regularly updated and enforced. Security policies should be tailored to the specific needs of the organization and its data. Security policies should be regularly reviewed and updated to ensure that they reflect the current threat landscape and prevent potential vulnerabilities. Secure server management for big data environments requires a comprehensive and detailed approach [13].

Organizations must have an effective security strategy in place, deploy the right security tools and policies, configure their systems properly, and regularly update their security policies. Doing so will ensure the confidentiality and integrity of the data and protect it from potential threats.

3. PROPOSED MODEL

Big data environments present unique security challenges due to their complexity, scalability, and heterogeneity. With the increase in the volume and variety of data, traditional security measures are no longer sufficient to protect data from unauthorized access. Implementing a secure server management system is essential for protecting big data environments. Secure server management systems provide a comprehensive approach to securing big data environments by leveraging a variety of tools, processes, and best practices.

These systems can be used to monitor, audit, and control access to data and servers, as well as to detect and respond to security threats. A secure server management system should incorporate a combination of controls to protect data, including access control, encryption, authentication, and auditing. Access control should be used to restrict who can access the data and what they can do with it. Encryption should be used to protect the data from unauthorized access and unauthorized modifications.

Authentication should be used to ensure that only authorized users can access the data. Finally, auditing should be used to track who has accessed the data and when. In addition to these security measures, a secure server management system should also include processes for managing and responding to security incidents. These processes should include procedures for identifying, reporting, and responding to security threats, as well as plans for how to recover from a security breach.

Finally, a secure server management system should include a set of best practices for ensuring the security of the big data environment. These best practices should include guidelines for configuring servers and networks, as well as for patching and updating software. They should also include processes for regularly testing and monitoring the security of the environment. Implementing a secure server management system is essential for protecting big data environments from unauthorized access and vulnerabilities. By leveraging a combination of tools, processes, and best practices, organizations can ensure that their data is secure, and their systems are protected.

Big data environments require secure server management to protect important data and resources. With the increasing amount of data being generated and stored, there is a greater need for secure server management to protect these valuable resources. To ensure secure server management, organizations must implement a series of security measures. First, organizations must ensure they have an effective authentication system in place to verify user identity and access rights. This can be accomplished by using strong passwords, requiring two-factor authentication, or implementing biometric authentication.

Additionally, organizations should also implement access control systems to restrict user access to data and resources. This can be done by using role-based access control or identity and access management systems. Organizations should also implement security measures to protect data in transit. This can be done by using encryption methods such as SSL/TLS and secure file transfer protocols. Additionally, organizations should also use firewalls and intrusion detection systems to detect and prevent malicious activities. Organizations should also implement regular security audits and vulnerability assessments to identify any security weaknesses.

This can help organizations quickly identify and fix any potential security issues. Additionally, organizations should also implement patch management systems to keep up with the latest security updates and patches. Finally, organizations should also develop and implement a data backup plan. This will help ensure that data is always available in case of a disaster or security

breach. Additionally, organizations should also develop and implement a disaster recovery plan to help ensure they can quickly respond to any security incidents. By implementing these security measures, organizations can ensure secure server management and protect their valuable data and resources.

4. RESULTS AND DISCUSSION

The proposed High-Performance Computing based optimization (HPCO) model has compared with the existing secure authentication and data sharing (SADS), authenticated key management scheme (AKMS), IoT-based big data secure management (IBDSM) and big data authentication in distributed environment (BDADE). Big data environments require secure server management in order to protect the data they store and process. In order to ensure that security is maintained, organizations must use several different methods to secure servers and protect data.

This will compare and contrast the various approaches to secure server management for big data environments. The first approach to secure server management for big data environments is authentication. Authentication is the process of verifying the identity of a user or device before granting access to a system. Organizations must ensure that authentication protocols are in place to ensure that only authorized users and devices have access to the data. The data security has demonstrated in Table.1.

Table.1. Comparison on Data Security

Inputs	**SADS**	**AKMS**	**IBDSM**	**BDADE**	**HPCO**
100	75.91	57.75	55.98	83.13	90.27
200	77.54	59.49	57.56	84.55	91.56
300	78.02	61.83	59.76	85.81	92.57
400	79.31	62.64	61.39	87.80	93.46
500	81.42	64.93	62.53	90.27	93.83
600	82.91	66.86	64.73	91.71	95.47
700	84.72	68.59	65.88	93.43	95.84

This can be accomplished by using multi-factor authentication, password less authentication, or other forms of strong authentication. The second approach to secure server management for big data environments is encryption. Encryption is the process of encoding data in such a way that it can only be accessed by authorized users.

Organizations must ensure that data is encrypted both in transit and at rest, in order to protect it from unauthorized access. This can be accomplished by using modern encryption algorithms such as AES, RSA, or Elliptic Curve Cryptography. The third approach to secure server management for big data environments is access control.

Access control is the process of restricting access to a system based on predefined user roles and privileges. Organizations must ensure that access control protocols are in place to ensure that only authorized users have access to the data. This can be accomplished by using role-based access control, attribute-based access control, or other forms of access control protocols. The comparison of big data management has shown in the Table.2.

Table.2. Comparison of big data management

Inputs	SADS	AKMS	IBDSM	BDADE	HPCO
100	74.53	58.22	53.63	79.94	94.43
200	74.42	58.24	53.46	79.67	93.93
300	74.40	59.12	54.19	79.97	94.05
400	77.50	61.95	57.53	83.48	97.28
500	78.70	63.27	58.26	84.80	97.66
600	79.31	64.10	59.15	85.34	98.23
700	79.72	64.50	59.23	85.64	97.93

The fourth approach to secure server management for big data environments is monitoring. Monitoring is the process of tracking user and system activity in order to detect and respond to any potential security threats. Organizations must ensure that monitoring protocols are in place to ensure that any suspicious activity is identified and addressed promptly. This can be accomplished by using log analysis, event correlation, or other forms of monitoring protocols.

In conclusion, secure server management for big data environments is a complex process that requires the use of various approaches. Organizations must ensure that authentication, encryption, access control, and monitoring protocols are in place in order to protect the data they store and process. By following these approaches, organizations can ensure that their data is secure and their systems remain secure. The comparison of server management has shown in the following Table.3.

Table.3. Comparison of server management

Inputs	**SADS**	**AKMS**	**IBDSM**	**BDADE**	**HPCO**
100	66.35	61.69	70.60	76.48	96.40
200	63.93	59.49	68.61	74.99	94.43
300	63.52	58.69	67.41	74.19	93.30
400	61.92	58.02	66.93	71.86	92.09
500	59.60	56.59	65.50	70.85	91.72
600	58.35	55.50	65.34	70.21	90.19
700	55.62	55.02	64.57	69.55	89.69

The performance analysis of secured server management for big data environments is an important problem that needs to be addressed. As more organizations move to the cloud for their data storage solutions, the need for secure and reliable server management solutions has become increasingly important. In order to ensure the security of the data stored in the cloud, organizations need to have a secure server management system in place. The first step in analyzing the performance of a secure server management system is to assess the security protocols that it uses. For example, organizations should make sure that they are using secure protocols such as SSL/TLS and SSH. These protocols will ensure that data is encrypted during transmission and that only authorized personnel can access the data.

Additionally, organizations should make sure that the server is configured to use strong authentication methods such as two-factor authentication and biometric identification. This will ensure that only authorized personnel can access the server. The next step in analyzing the performance of a secure server

management system is to assess the performance of the server itself. This includes assessing the server's uptime, response times, and scalability. Organizations should make sure that the server is always available and has the capacity to handle the demands of the organization's big data environment.

Organizations should make sure that the server is configured to use the latest security protocols and encryption methods to protect the data stored on the server. Finally, organizations should assess the performance of the server's logging and monitoring systems. Logging and monitoring systems can be used to detect any unauthorized access or activity on the server. The comparison of logging and monitoring systems is shown in the Table.4.

Table.4. Comparison of logging and monitoring systems

Inputs	SADS	AKMS	IBDSM	BDADE	HPCO
100	69.82	69.39	68.66	73.67	90.14
200	69.71	68.89	68.66	72.58	89.88
300	69.65	68.14	67.83	71.44	89.31
400	69.60	68.14	68.56	71.80	90.45
500	69.56	69.19	69.67	73.33	91.47
600	69.53	69.47	70.07	73.97	91.71
700	69.51	68.75	69.50	73.39	91.06

This information can then be used to help organizations identify and respond to security incidents in a timely manner. Additionally, organizations should ensure that the logging and monitoring systems are configured to send alerts when potential security incidents occur. The performance analysis of secured server management for big data environments is essential for organizations to ensure the security of their data and their servers. Organizations should use a combination of security protocols, server performance measures, and logging and monitoring systems to ensure that the server is secure and reliable. By doing so, organizations can ensure that their data is secure and that the server is performing properly.

Big data environments are becoming increasingly complex and data-intensive. As a result, the performance optimization of secured server management for these environments is becoming more important. The challenge is to ensure that the server is secure and efficient, while also providing the necessary capabilities to manage the big data environment. In order to optimize the performance of secured server management for a big data environment, a number of measures should be taken. First, the system should be designed with security in mind. This includes ensuring that data is encrypted and secure, and that access is restricted to only those who are authorized. Additionally, the system should be regularly monitored and updated to protect against potential vulnerabilities or attacks.

Second, the system should be designed to be highly available and scalable. This means that the system should be able to handle large amounts of data without any latency issues. This can be achieved by using techniques such as clustering, replication, and distributed computing. Additionally, the system should be able to quickly respond to requests and process data in real-time. Third, the system should be designed to optimize the performance of the big data environment. This includes ensuring that the system can handle large amounts of data and that data is processed quickly and efficiently. Additionally, the system should be able to utilize the resources of the environment efficiently, such as the storage and processing power.

5. CONCLUSION

The organizations should regularly review their server security policies and procedures to ensure that they are up to date and compliant with current security best practices. The organizations should ensure that their server management system is regularly monitored and tested for vulnerabilities. This can be done using vulnerability scanning software or by hiring a third-party security firm to audit the system for any potential weaknesses. Organizations should also make sure that their server management system is regularly updated with the latest security patches and updates. The secure server management is essential for any organization managing sensitive data. By implementing the right security measures and regularly monitoring and testing the system, organizations can ensure that their data is safe and secure. Finally, the system should be designed to be reliable and resilient. This includes ensuring that the system is able to recover from any potential failure or outage quickly and without disruption. Additionally, the system should be able to handle any changes or updates that are necessary without any downtime. By taking these measures, the performance optimization of secured server management for big data environments can be achieved. In this way, organizations can ensure that their systems are secure, efficient, and reliable, while also providing the necessary capabilities to manage the big data environment.

REFERENCES

[1] U. Narayanan, V. Paul and S. Joseph, "A Novel System Architecture for Secure Authentication and Data Sharing in Cloud Enabled Big Data Environment", *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 6, pp. 3121-3135, 2022.

[2] T.S. Algaradi and B. Rama, "An Authenticated Key Management Scheme for Securing Big Data Environment", *International Journal of Electrical and Computer Engineering*, Vol. 12, No. 3, pp. 3238-3239, 2022.

[3] C.L. Stergiou and B.B. Gupta, "IoT-Based Big Data Secure Management in the Fog over a 6G Wireless Network", *IEEE Internet of Things Journal*, Vol. 8, No. 7, pp. 5164-5171, 2020.

[4] P.P. Sharma and C.P. Navdeti, "Securing Big Data Hadoop: A Review of Security Issues, Threats and Solution", *International Journal of Computer Science and Information Technologies*, Vol. 5, No. 2, pp. 2126-2131, 2014.

[5] M. Wazid and J.J. Rodrigues, "Authentication in Cloud-Driven IoT-based Big Data Environment: Survey and Outlook", *Journal of Systems Architecture*, Vol. 97, pp. 185-196, 2019.

[6] D. Shin and R. Gajanayake, "Secured E-Health Data Retrieval in DaaS and Big Data", *Proceedings of IEEE International Conference on E-Health Networking, Applications and Services*, pp. 255-259, 2013.

[7] N. Abdullah and E. Moradian, "Blockchain based Approach to Enhance Big Data Authentication in Distributed Environment", *Proceedings of IEEE International*

Conference on Ubiquitous and Future Networks, pp. 887-892, 2017.

[8] G. Manogaran and C. Thota, "A New Architecture of Internet of Things and Big Data Ecosystem for Secured Smart Healthcare Monitoring and Alerting System", *Future Generation Computer Systems*, Vol. 82, pp. 375-387, 2018.

[9] D.S. Terzi and S. Sagiroglu, "A Survey on Security and Privacy Issues in Big Data", *Proceedings of IEEE International Conference on Internet Technology and Secured Transactions*, pp. 202-207, 2015.

[10] A. Kumari and N. Kumar, "Blockchain-Based Massive Data Dissemination Handling in IIoT Environment", *IEEE Network*, Vol. 35, No. 1, pp. 318-325, 2020.

[11] N. Jiwani and K. Gupta, "Exploring Business Intelligence Capabilities for Supply Chain: A Systematic Review", *Transactions on Latest Trends in IoT*, Vol. 1, No. 1, pp. 1-10, 2018.

[12] J. Lloret and J. Tomas, "An Architecture and Protocol for Smart Continuous eHealth Monitoring using 5G", *Computer Networks*, Vol. 129, pp. 340-351, 2017.

[13] N. Jiwani and K. Gupta, "Comparison of Various Tools and Techniques used for Project Risk Management", *International Journal of Machine Learning for Sustainable Development*, Vol. 1, No. 1, pp. 51-58, 2019.