[5] Jianfeng Zhou, Genserik Reniers , Valerio Cozzani. A Petri-net approach for firefighting force allocation analysis of fire emergency response with backups. //Reliability Engineering & System Safety. Volume 229, January 2023, pp. 108847.
[6] Нестеров Р.А., Савельев С.Ю. Генерация сетей Петри с помощью структурных трансформаций, сохраняющих поведенческие свойства. // Труды Института системного программирования РАН. 2021; 33(3): 155-170. https://doi.org/10.15514/ISPRAS-2021-33(3)-12
[7] Серебренников К.Г. Вычисление приоритетов срабатывания переходов для живых сетей Петри. // Труды Института системного программирования РАН. 2019;31(4):163-174. https://doi.org/10.15514/ISPRAS-2019-31(4)-11
[8] Учайкин Р.А. Сравнительная оценка эффективности компьютерной техники в подразделениях промышленного предприятия / Р.А. Учайкин, С.П. Орлов // Вестник Самарского государственного технического университета. – 2020. – № 1 (65). – С. 74–86.
[9] Самойлов П.А. Методика разработки и внедрения комплексных решений автоматизации проектирования и производства изделий машиностроения: автореферат диссертации на соискание ученой степени кандидата технических наук: 05.13.12./Самойлов Павел Александрович. – Оренбург, 2021. - 16 с.
[10] Орлов С.П. Применение моделей на сетях Петри при организации технического обслуживания автономных агротехнических транспортных средств/ С.В. Сусарев, С.П. Орлов, Е.Е. Бизюкова, Р.А. Учайкин// Известия Санкт-Петербургского государственного технологического института (технического университета)». – 2021. – Вып. № 58(84). – С. 98-104. DOI: 10.36807/1998-9849-2021-58-84-98-104
[11] Кизим, А. В. Модели и методы интеллектуальной поддержки принятия решений при управлении процессом технического обслуживания, ремонта и модернизации промышленного оборудования: дис. д-ра техн. наук: 05.13.01/Кизим Алекаей Владимирович. – Волгоград, 2021. – 289 с.

Investigating security issues in a big data environment

Latafat Gardashova, Farid Naghiyev
Azerbaijan State Oil and Industry University

Abstract
Security in a big data environment covers important issues such as data protection, security analysis, authentication, accessibility security and data recovery policies. Research in this area is important for ensuring information security and developing security standards. Strong encryption, user authentication, and data recovery processes help improve security and reduce security risks in big data environments.
Key words: Big Data, Data Security, Data Leakage, Firewalls, Authentication, Data Encryption

Introduction

The rapidly evolving face of the digital age has become defined by the concept of big data. Millions of data points are created and processed every day, affecting almost every aspect of businesses, institutions, and even individuals. However, despite the many benefits brought by this abundance of data, it also comes with serious security concerns. Big data is much more than just a concept consisting of numbers, texts and graphics. This refers to a processing-intensive, diverse, and often dynamic dataset that contains potentially sensitive information. However, as this massive amount of data is processed and stored, privacy breaches, data manipulation and other security threats are increasingly occurring. In this article, we will focus on security issues in the big data environment. The likelihood of businesses and individuals encountering these issues is increasing day by day, and therefore it is vital to pay attention to this issue. While we evaluate the opportunities offered by big data, we also need to take the necessary steps to protect data security and integrity.

As we take an in-depth look at security challenges in the big data environment, we will understand current threats and identify best practices. In conclusion, we hope this article guides readers on the path to ensuring security in the world of big data.

What is Big Data?

Big data refers to the large amount of data produced and stored in the digital world today. This data may be of sizes that cannot be managed with traditional data storage and processing methods. Big data is defined through three key characteristics: volume, variety, and velocity.

Volume: Big data includes amounts of data that traditional data storage systems cannot handle. This means throughput in the order of terabytes, petabytes and even zetabytes.

Diversity: Big data can include data from different sources and in different formats. It contains various types of data such as text, audio, images, video.

Speed: Big data is often generated and processed very quickly. Ever-increasing data sources, such as real-time data streams and data from IoT (Internet of Things) devices, increase the speed of large data sets. Big data contains valuable information that helps businesses, governments, and researchers improve decision-making processes. By enabling the extraction of meaningful information from these data sets, big data analytics can be applied in a wide range of areas, from analysis of market trends to optimization of patient treatment. The power of big data allows businesses to gain competitive advantage, governments to improve services, and to expand the frontiers of science. However, security and privacy challenges encountered during the management and analysis of big data should also be taken into account.

Security Issues in Big Data Environment

While big data offers many opportunities for businesses and individuals, it also brings serious security challenges. Security issues in the big data environment arise in areas such as data confidentiality, data integrity, data access and authorization and include various security threats.

Data Privacy : In a big data environment, collecting and storing personal and sensitive information increases privacy issues. If this information is subject to unauthorized access or is intercepted by malicious individuals, serious consequences may occur. Data privacy is of great importance, especially in areas where sensitive data types are processed, such as the healthcare sector. Data Integrity : In a big data environment, data integrity is the process of ensuring that data has not been modified and its accuracy is maintained. Violation of data integrity may result in data being manipulated or altered, which may lead to incorrect decisions or security breaches. Data Access and Authorization : In big data systems, access and authorization of data poses a significant security challenge. Businesses must develop effective authentication and authorization mechanisms to ensure that only authorized individuals have access to data. Additionally, data access permissions should be reviewed regularly and unnecessary access should be restricted. 4. Data Reliability: In the big data environment, the reliability of data is a major concern. Uncertainties about the source and accuracy of data can lead to wrong decisions and exploitation of security vulnerabilities. To ensure data reliability, data sources should be regularly checked and data quality assured. Security of Big Data Analytics : Big data analytics processes involve security risks when processing and analyzing data. There may be an increased risk of malicious attacks or data manipulation, especially when complex analytical techniques such as machine learning and artificial intelligence are used. Therefore, the security of big data analytics requires careful auditing of processes and algorithms. Security issues in the big data environment are a significant challenge faced by businesses and individuals. To deal with these problems, effective security policies and technological solutions must be developed and implemented. In addition, increasing security awareness and organizing security training is also of great importance.

Security Hazards in the Big Data Environment

In the big data environment, data abundance and complexity bring various security threats. These threats can impact fundamental security principles such as data confidentiality, integrity and access. Here are

the security dangers frequently encountered in the big data environment Data Leak : In a big data environment, there is a risk that data may fall into the hands of unauthorized persons or be leaked as a result of unauthorized access. This can be done by hackers, internal threats, or malicious employees. Data leakage can result in reputational damage, legal issues, and financial losses for organizations.

Data Theft and Attacks : Valuable information stored in the big data environment becomes a potential asset that can be targeted. Hackers or malicious groups can access this data and steal or damage it. Data theft and attacks can seriously affect the reputation and financial health of businesses.

Data Manipulation : The complexity of large data sets makes it easy to manipulate the data. Malicious actors may modify data for misleading or harmful purposes. This can lead to wrong decisions, exploitation of vulnerabilities, or loss of reputation.

Distributed Denial of Service Attacks (DDoS) : Big data systems are often accessible via the internet and can be subject to online attacks. Distributed Denial of Service Attacks (DDoS) overload a service or network, preventing access and stopping systems from functioning. These attacks can seriously impact the availability of big data systems.

Data Security Weaknesses : Big data systems are often complex and large-scale, increasing potential security vulnerabilities. Software bugs, poorly configured security settings, or unupdated systems can make it easier for malicious actors to infiltrate systems.

These security hazards pose a significant challenge to protecting data in a big data environment. Businesses need to deal with these dangers by taking measures such as effective security policies, firewalls, strong authentication systems and regular security audits. In addition, it is important to increase the security awareness of employees and organize continuous security training.

Best Practices for Big Data Security

Big data security involves a set of best practices and strategies to protect and secure the data assets of businesses and organizations. Here are important best practices for big data security : Data Encryption : Encrypting sensitive data plays a fundamental role in protecting data privacy. Data encryption ensures the security of data during storage, transmission and processing. Encrypting both dynamic and static data provides an additional layer against unauthorized access. Firewalls and Network Monitoring : Firewalls and network monitoring systems monitor and filter network traffic for malicious attempts. These systems detect and block unauthorized access attempts, thus helping to protect data. Authorization and Authentication : Effective authorization and authentication mechanisms should be used to control access to data. Strong authentication methods, such as dual-factor authentication, prevent unauthorized access to data.

Security Training and Awareness : It is important to train and raise awareness of employees on security issues. Safety training helps employees understand safety policies and develop safe work habits. Data Analytics Security : During big data analytics processes, data security should be at the forefront. Security controls must be integrated to ensure the security of algorithms and analysis processes. Additionally, appropriate auditing mechanisms should be used to ensure the accuracy and reliability of data analytics results.

Data Backup and Recovery : Data backup and recovery processes should be performed regularly in large data systems. This prevents data loss and ensures access to data in the event of possible security breaches or system failures. Continuous Security Assessments : Regular security assessments should be conducted to ensure the security of big data systems. These assessments help identify and remediate vulnerabilities so that data security is continually strengthened. These best practices for big data security provide essential guidance for businesses and organizations to protect and secure their data assets. Regular review and updating of these applications ensures ongoing protection against security threats.

Future Perspectives

As big data technologies and applications continue to develop rapidly, significant changes and developments are expected in the field of big data security. Here are future perspectives in the field of big data security :

Strengthening Security with Machine Learning and Artificial Intelligence :

Machine learning and artificial intelligence have begun to play an important role in the field of big data security. These technologies can be used to detect abnormal activities, prevent threats, and close security vulnerabilities in big data systems. In the future, these technologies are expected to be further developed and disseminated. Internet of Things (IoT) Security : The rapidly increasing number of IoT devices poses new challenges for big data security. In the future, stricter standards and regulations regarding the security and data privacy of IoT devices are expected. Additionally, it is important to develop and implement new technologies for the security of IoT devices.

Use of Blockchain Technology : Blockchain technology also has significant potential in the field of big data security. Distributed ledger technology enables data to be stored and tracked securely. In the future, blockchain-based solutions are expected to be used more for big data security. Biometric Authentication : Biometric authentication technologies can be an important tool for improving security in big data systems. Biometric technologies such as fingerprint recognition, facial recognition, and voice recognition can be used as strong authentication methods. In the future, these technologies are expected to be more widely adopted and integrated.

More Advanced Encryption Methods : Data encryption technologies are constantly being developed and strengthened. In the future, stronger and more complex encryption algorithms and methods are expected. This can provide a higher level of protection regarding data privacy and security.

Future perspectives in the field of big data security are a reflection of technological advances and changing security needs. These perspectives provide important guidance for strengthening the security of big data systems and being prepared for new threats that may arise in the future.

Conclusion

Big data is one of the greatest assets businesses and organizations face in today's digital age. However, this abundance of big data brings with it a number of security challenges. Data leakage, data manipulation, distributed denial-of-service attacks, and other security threats pose a significant challenge to protecting data in the big data environment. In this article, we examined security issues in the big data environment and discussed various security hazards and best practices. Best practices such as data encryption, firewalls, strong authentication, and ongoing security assessments are important steps to secure big data systems. In future perspectives, new technologies such as machine learning, artificial intelligence, blockchain technology and biometric authentication are expected to play an important role in the field of big data security. These technologies can further increase the security of big data systems and enable us to be better prepared against new threats that may arise in the future. As a result, big data security will continue to be a key priority for businesses and organizations to protect and secure their data assets. Increasing security awareness, using up-to-date technologies, and continuous security assessments are essential steps to strengthen the security of big data systems.

References:

[1] https://hevodata.com/learn/big-data-security/
[2] https://www.instinctools.com/blog/big-data-security-concerns/
[3] https://www.cprime.com/resources/blog/big-data-security-biggest-challenges-and-best-practices/
[4] https://www.dataversity.net/big-data-security-challenges-and-solutions/
[5] https://www.datamation.com/big-data/big-data-security/
[6] https://www.sas.com/en_us/insights/big-data/what-is-big-data.html
[7] https://www.xenonstack.com/blog/big-data-security
[8] https://www.kdnuggets.com/2016/06/5-best-practices-big-data-security.html