Securing Big Data Through Cybersecurity

[1]Shaik Asrar

PG Scholar, Department of MCA
Dayananda Sagar College of Engineering
Bangalore, India
asrarshaik001@gmail.com

[2]Alamma B.H

Assistant Professor Department of MCA
Dayananda Sagar College of Engineering
Bangalore, India
alamma-mcavtu@dayanandasagar.edu

***Abstract*—The paper emphasizes the need for fast coordination and emergency response plans in the event of a cyberattack. The paper also highlights the importance of security incident and event management (SIEM) for fraud detection and network protection. The paper also discusses the importance of visual analytics in providing an environment to visualize and analyze data to gain insights. Finally, the paper provides strategies and best practices for ensuring the security of big data within the cybersecurity landscape.**

In this paper we discuss about the developing centrality of huge information in different segments, highlight the potential dangers and vulnerabilities related with its capacity and investigation, and propose techniques and best hones to address the complex assignment of securing enormous information within the cybersecurity scene.

***Keywords*—Security Issues Of Big Data, Defense-in-depth concept, Threat intelligence and information sharing, Data Encryption, Detection, Prevention, Response to Cyberattacks.**

I. INTRODUCTION

Big data refers to very large and complex data that is difficult to manage, process, or analyze using traditional data processing methods. It has huge data, high speed and a wide variety of files.

Cybersecurity means the practice of protecting computer systems, networks and information from unauthorized access, use, disclosure, destruction, alteration or destruction. This includes implementing measures and controls to prevent, detect and respond to cyber threats, including malicious attacks, inaccessibility, data exfiltration and other cybercriminal activities.

Protection of big data in cybersecurity refers to the practices, measures and procedures used to protect big data from inaccessibility,destruction, theft or any kind of damage in the context of cybersecurity. Big data generally refers to a large amount of information produced, collected and stored by organizations, often in different formats and from different sources.

In the era of digital transformation, organizations are generating and collecting vast amounts of data at an unprecedented rate. This exponential data growth, commonly known as Big Data, has revolutionized industries by enabling data-driven decision-making, personalized experiences, and improved work efficiency.

The security of big data has become a pressing issue in network security. The scaleand complexity of big data presents unique challenges that security measures have always had to overcome. Securing big data requires a multifaceted approach in the enterprise that includes technology development, a strong security framework, effective data management and cybersecurity leadership. Threat intelligenceplatforms require the integration of advanced technologies such as machine learning algorithms and advanced encryption techniques.

OBJECTIVE

The Objective of this research paper is to explore the challenges and solutions for protecting big data from cyber threats.

The purpose of this article is to provide ideas and strategies to better understand the specific security issues associated with big data and ensure that this data remains confidential, informational, integrity and availability.

II. LITERATURE SURVEY

In the paper the authors emphasize the need for a scientific approach to managing big data and reducing security risks. Case studies suggest strategies to support development of personal protective equipment as well as big data detection and protection systems. It also highlights the importance of combining implementation processes with policies and regulations to better address big data and privacy concerns. The advent of big data has opened up new avenues for business and investment. However, there are still serious security risks that require accurate and thorough analysis.[1]

In the paper the authors highlights the importance of security and event management (SIEM) for fraud detection and network protection. It also highlights the need to create a system that can collect and interact with different data to present it on a data scientist's dashboard. The use of big data visualization and analysis techniques can be useful for analyzing network traffic data and conducting post-analysis studies. This article proposes to develop a system that uses big data to provide forensic information to forensic experts and reduce the time and cost of forensic analysis. The research focuses on advanced data mining tools and techniques related to big data analytics.The article also discusses the importance of visual analysis in providing an environment for visualization and analyzing data for visualization.[2]

In the paper the authors demonstrates the increasing integration of various knowledge-generating technologies into healthcare and knowledge development. However, security and privacy concerns are great and hospitals cannot use the data with existing resources. This article presents the issues of government security and privacy in big data as it applies to healthcare, and discusses data privacy, data security, use of people's access to procedures, and policies.[3]

In the paper the authors emphasize the importance of evidence describing where the information came from and how it developed in order to evaluate the reliability of information. The article also illustrates the need for large-scale word processing datasets and various types of features that can be used to characterize Weibo messages. Data science is said to combine techniques from various disciplines, including natural language processing, data mining, machine learning, relational analysis, and paper data mining, into a guide to spotting misinformation on the Internet.[4]

In the paper the authors This paper discusses the continued digitization of commercial and non-commercial organizations driving the growth of big data analytics. IoT devices collect data from various fields such as health, energy, weather, business, transportation, education and manufacturing. Big data, often referred to as "big data", is collected, extracted, analyzed and visualized to reveal behavior and patterns to inform decision making. One challenge with big data is storing and analyzing collected data, providing timely insight and speeding up decision making.[5]

III. SECURITY ISSUES OF BIG DATA

A. Advanced Persistent Threats (APTs): Big data environments are good targets for cyberattacks, including APTs. APTs are advanced, long-term programs designed to compromise systems and gain access to sensitive information. Data breach and theft: Big data environments can contain a lot of sensitive information. Attackers can try to use vulnerabilities to access and steal this information.

B. Distributed heterogeneous data sources: Big data environments often contain distributed data sources, including data from multiple systems, applications, and other sources.

C. Scalability and performance impact: Traditional security solutions can tackle large data volumes and manage data volume and speed. Security Analysis and Machine Learning: Use advanced analytics and machine learning techniques to analyze large volumes of data and identify patterns or anomalies that may indicate a security breach threat. This technology helps identify unknown or advanced cyberattacks, predict potential threats, and perform threat hunting.

D. Dynamic and Evolving Threat Landscape: The cyber threat landscape is constantly changing, with new attacks, techniques, and vulnerabilities constantly emerging.

E. Lack of Monitoring: The big data environment generates large volumes of data and events, making it difficult to monitor and analyze the security status.

IV. METHODOLOGY

A. Technologies for securing Big data through Cybersecurity

1. Authentication and access control: Use technologies such as multi-factor authentication (MFA), identity and access management (IAM), and role management (RBAC) to identify users and control access to large files. This technology ensures that only authorized persons can access and manage data.

2. Encryption: Encryption techniques are required to protect sensitive information. By transforming data into an unreadable form, they can ensure that data remains protected even if tampered with or damaged Encryption can be used for data at rest (stored data) and data in transit (data transferred from the machine).

Figure 1: The Process Of Data Encryption

3. Intrusion Detection and Prevention System (IDPS): IDPS technology monitors network connections, system events, and user activity to identify and respond to potential cyber threats. They use signature-based detection, stealth detection, and behavioral analysis to detect malicious activity, including big data attacks.

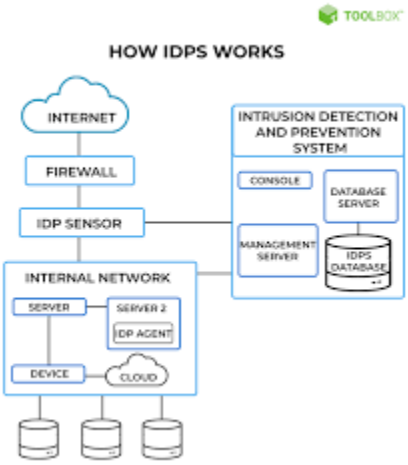

Figure 2: The Working of IDPS

4. Data desensitization and anonymization: Adopt data desensitization and anonymization technology to protect sensitive data in big data. These technologies transform or anonymize data, enabling organizations to use personally identifiable information for development, testing and analysis without disclosing Personal Information (PII).

B. Methods for securing Big Data

1. Defense-in-depth concept: Use a layered approach to security by combining multiple security controls at multiple levels. This includes network security, access control, access, access and protection systems (IDPS), endpoint security, and security monitoring. Organizations can reduce the impact of a successful cyberattack by having multiple layers of protection.

The technology is used by "Financial Institutions" that manage large amounts of customer data and are at high risk of cyberattacks. They use defense-in-depth strategies to protect their networks, systems, and customer data. This strategy includes the integration of multiple layers of security management and technology.

Figure 3: Layers Of Defense In Depth Architecture

2. Threat intelligence and information sharing: Stay informed about the latest cyber threats, attacks and vulnerabilities with threat intelligence from a trusted source. Participate in industry knowledge- sharing programs and collaborate with peers to gain insights and improve defenses.

Sharing threat information can help organizations better identify and respond to emerging threats.

The technology is used in cybersecurity information sharing and analysis centers (ISACs), which are industry-specialized organizations that help share threat and cyberattack information among organizations in a specific location. For example, Financial Service ISAC (FS- ISAC) works in financial institutions to report cyber threat information in real time.

3. Data Encryption: Encrypt sensitive data at rest and in transit to prevent unauthorized access.Encryption ensures that data cannot be read by unauthorized persons, even if it is compromised.

In business and finance, financial transactions, customer information and personal information are constantly exchanged between financial institutions, payment systems and merchants. Data encryption is used to protect communications from unauthorized interference or tampering.

V. DISCUSSION

A. *Detection:*

Analyzing cyberattacks in a big data environment requires a multidisciplinary approach. Advanced cybersecurity technologies such as mystery detection and behavior analysis play an important role. By analyzing patterns and behavior in large volumes of data, these technologies can identify differences in normal activities that could indicate potential cyberattacks.

B. *Prevention:*

Preventing cyberattacks in the big data environment requires effective cybersecurity strategies. Start by implementing strong controls and authentication procedures to ensure that only authorized users can access sensitive information. Encryption should be used to protect data at rest and in transit to reduce the risk of unauthorized access or data breach.

Provide a training program to teach employees cybersecurity best practices, such as creating strong passwords, identifying phishing emails, and avoiding malicious downloads or links. These practices are continually promoted to foster a culture of security awareness in the organisation.

C. *Response:*

Cyberattacks in the big data environment require fast coordination. Once an attack is detected, immediate steps must be taken to isolate the affected system and limit the attacker's access. An emergency response plan should be activated, including a well- prepared emergency response team, after specified evacuation and rescue procedures. Forensic analysis should be performed to determine the extent of the attack, identify potential use, and gather evidence for legal or investigative purposes.

VI. CONCLUSION

In conclusion, in today's data-driven world, protecting big data through cybersecurity is crucial. Big data presents unique challenges due to its volume, speed and diversity, making it a prime target for cyberattacks But with the right ideas, strategies, and practices, organizations can protect big data from threats.

The defense-in-depth concept combines multiple security controls and technologies to provide a solid foundation for protecting big data. This approach includes authentication and access control, encryption, data desensitization and anonymization, access detection and protection, and security measures. Using this technology, organizations can build a defense against cyber threats and manage the privacy, integrity, and availability of big data.

REFERENCES

1. Su Chunli, “Big Data Security and Privacy Protection”, International Conference on Virttual Reality and Intelligent Systems (ICVRIS), 2019.
2. Bipin Bihari, M.R.Patra, D Bhanu Mahesh, “SECURITY ISSUES AND CHALLENGES OF BIG DATA ANALYTICS AND VISUALIZATION”,CVR College of Engineering, 2016.
3. Karim ABOUELMEHDI, “Big data security and Privacy in healthcare” A review, International Conference on Emerging Ubiquitous Systems and Private Networks(EUSPN), 2017.
4. Xu, Lei, Chunxiao Jiang, Jian Wang, Jian Yuan, and Yong Ren. "Information security in big data: privacy and data mining." Ieee Access 2 (2014): 1149-1176.
5. Yang, Longzhi, Jie Li, Noe Elisa, Tom Prickett, and Fei Chao. "Towards big data governance in cybersecurity." Data-Enabled Discovery and Applications 3 (2019): 1-12.
6. Alani, Mohammed M. "Big data in cybersecurity: a survey of applications and future trends." Journal of Reliable Intelligent Environments 7, no. 2 (2021): 85-114.
7. Rawat, Danda B., Ronald Doku, and Moses Garuba. "Cybersecurity in big data era: From securing big data to data-driven security." IEEE Transactions on Services Computing 14, no. 6 (2019): 2055-2072.