Managing Security, Privacy and Ethical Risks Associated with Big Data and Predictive Analytics Applications

Luka Novak
Information Security, University of Ljubljana

Eva Zupančič
Business Ethics, University of Ljubljana

Keywords:

- big data
- predictive analytics
- machine learning
- security
- privacy
- ethics

Excellence in Peer-Reviewed Publishing:
QuestSquare

Abstract

Big data analytics offers valuable insights but also poses risks surrounding security, privacy, and ethics that must be addressed. This research reviews the nature of big data and predictive analytics, then analyzes key security risks including increased attack surfaces, data breaches, weak access controls, and poor encryption. Technical security controls are proposed such as network segmentation, role-based access, encryption, API security, data auditing, and penetration testing. Privacy risks are also examined, including personal data exposure, behavioral profiling, lack of consent, and erosion of anonymity. Privacy controls include consent, anonymization, data minimization, and transparency about practices. On the ethics front, issues like opacity of models, flawed data, reinforcing bias, discrimination, manipulation of users, and loss of human discretion are discussed. Ethical principles are suggested, including explain ability, fairness, accountability, empowerment, auditability, and human oversight of analytics. Tables summarize the security, privacy, and ethics controls. In conclusion, while big data analytics delivers value, managing the accompanying security, privacy and ethical risks is crucial for its responsible use. Diligent technical and policy measures on security, consent-based privacy, and ethical oversight will allow organizations to harness big data analytics in a socially beneficial way.

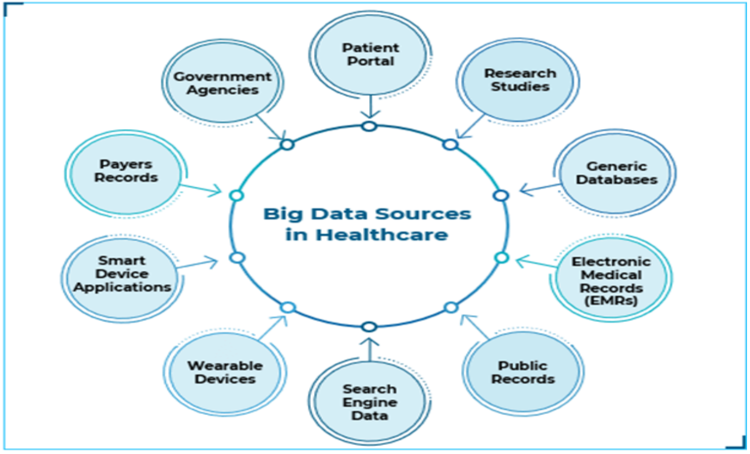
Introduction

The proliferation of big data and predictive analytics in contemporary organizational landscapes has emerged as a transformative force, providing unprecedented opportunities for insights and enhanced decision-making capabilities. Organizations across diverse sectors have increasingly leveraged these technologies to extract valuable patterns and trends from vast datasets, thereby gaining a competitive edge in their respective domains. However, the pervasive adoption of big data and predictive analytics is not without its challenges. This research article undertakes a comprehensive investigation into the inherent security, privacy, and ethical risks associated with the implementation of these technologies. In doing so, it aims to elucidate the critical considerations that organizations must address to navigate the complex landscape of big data and predictive analytics responsibly [1]. In the contemporary landscape of information technology, the convergence of big data and predictive analytics has ushered in a paradigm shift, augmenting the scope and complexity of vulnerabilities in various domains. One of the foremost concerns pertains to security, with the burgeoning volume of data susceptible to unauthorized access, data breaches, and potential exploitation. The intricate interplay of interconnected systems and the vast repositories of sensitive information demand meticulous attention to safeguard against malicious activities that could compromise the integrity of data and undermine the overall security framework [2].

Simultaneously, the exponential growth in data collection and analysis raises profound privacy concerns [3]. The amalgamation of diverse datasets for predictive purposes introduces the challenge of preserving the confidentiality of individuals' personal information. As organizations leverage big data to extract valuable insights, the boundaries between data utilization for legitimate purposes and potential privacy infringements become increasingly blurred. Consequently, there is a pressing need to establish robust privacy frameworks that balance the imperative of data-driven decision-making with the protection of individual privacy rights.

Ethical considerations further amplify the intricacies associated with the deployment of predictive analytics. The potential for bias in algorithms, leading to unfair or discriminatory outcomes, is a critical ethical concern. Decision-making models trained on historical data may inadvertently perpetuate existing biases, exacerbating societal inequities [4]. Ensuring fairness in predictive analytics demands a meticulous examination of the algorithms and datasets used, necessitating the development of strategies to identify, rectify, and prevent bias in decision-making processes. Moreover, transparency in the deployment of predictive analytics is imperative to engender trust among stakeholders, allowing for a more informed evaluation of the ethical implications associated with algorithmic decision-making [5].

Figure 1.



This research aims to dissect these multifaceted challenges, offering a comprehensive analysis of the potential consequences stemming from the integration of big data and predictive analytics. The exploration encompasses not only the technical dimensions of security and privacy but also delves into the ethical considerations that underpin responsible data usage [6]. To address these challenges effectively, pragmatic strategies are proposed, emphasizing the importance of robust cybersecurity measures to fortify data integrity and thwart unauthorized access. Additionally, the research advocates for the implementation of privacy-preserving technologies and stringent regulatory frameworks to safeguard individuals' personal information in the era of big data. Furthermore, the research underscores the significance of ethical guidelines and governance mechanisms to navigate the intricate ethical landscape associated with predictive analytics. This involves promoting transparency in algorithmic decision-making, fostering fairness through continuous monitoring and refinement of algorithms, and instituting mechanisms to rectify biases as they emerge. By unraveling the complexities of these challenges and offering practical solutions, this research seeks to contribute to the development of a resilient framework that harnesses the potential of big data and predictive analytics while mitigating the associated risks in a manner that aligns with ethical standards and societal expectations [7].

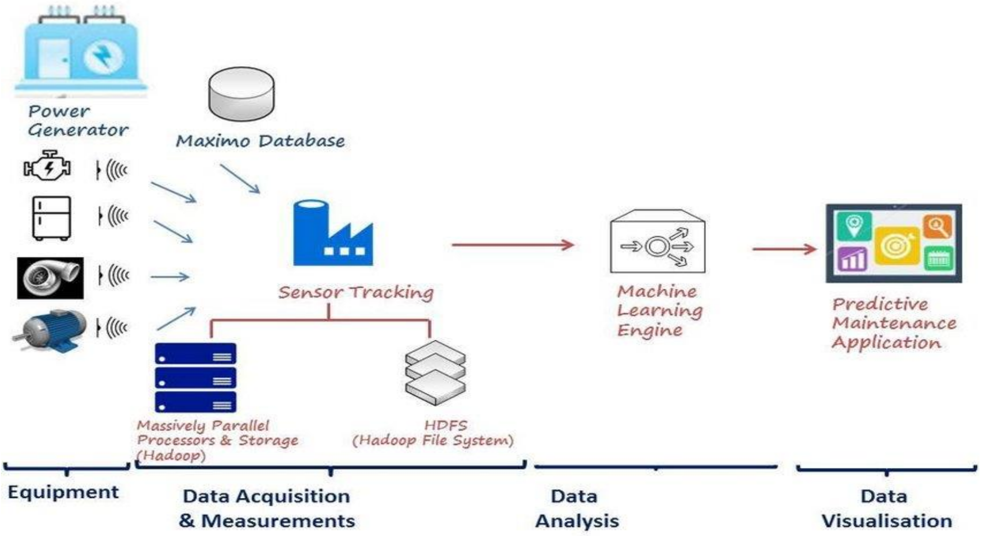
Against this backdrop, the significance of establishing robust frameworks for managing the security, privacy, and ethical dimensions of big data and predictive analytics cannot be overstated [8]. The research delves into existing literature and case studies to distill key principles and best practices for organizations seeking to implement these technologies responsibly [9]. By synthesizing a comprehensive understanding of the risks involved, this article aims to equip decision-makers, data scientists, and policymakers with actionable recommendations to navigate the intricate landscape of big data and predictive analytics securely and ethically.

Defining Big Data and Predictive Analytics

Big data represents the paradigm shift in the way we handle and analyze data. It encompasses vast and intricate datasets that defy conventional data processing methods due to their sheer volume, velocity, and variety. The enormity of the data sets is a defining characteristic, posing significant challenges to traditional analytical approaches. The volume of data is substantial, often reaching levels that are impractical to manage using conventional tools. Simultaneously, the velocity at which data is generated and updated is unprecedented, requiring real-time or near-real-time processing capabilities. Additionally, big data exhibits a high degree of variety, originating from diverse sources in both structured and unstructured formats. The continuous influx of data further complicates the scenario, necessitating advanced technologies and methodologies for effective analysis and extraction of meaningful insights.

Predictive analytics emerges as a powerful ally in the realm of big data. It involves the application of sophisticated techniques to scrutinize current and historical data, unraveling patterns and trends that lay the groundwork for predicting future events and behaviors. The core objective is to discern correlations and relationships within the data, leveraging statistical models and machine learning algorithms. A broad spectrum of methods falls under the umbrella of predictive analytics, encompassing regression analysis, forecasting, machine learning algorithms, data mining, game theory, and optimization strategies [10]. By deciphering the complex web of data, organizations can anticipate future developments, enabling informed decision-making and proactive responses.

Figure 2.


Power Generator
Maximo Database
Sensor Tracking
Machine Learning Engine
Predictive Maintenance Application
Massively Parallel Processors & Storage (Hadoop)
HDFS (Hadoop File System)
Equipment
Data Acquisition & Measurements
Data Analysis
Data Visualisation

The synergy between big data and predictive analytics is pivotal for organizations aiming to extract maximum value from their data reservoirs. The marriage of these two concepts empowers entities to unveil subtle trends and patterns that remain elusive in smaller datasets [11]. The insights derived from this fusion serve diverse purposes, ranging from predicting customer churn to optimizing supply chains and even detecting fraudulent activities. The transformative potential is immense, revolutionizing the way businesses operate and make strategic decisions. However, the efficacy of this synergy hinges on the quality of both the data and the predictive models employed. Ensuring the reliability of results demands a rigorous commitment to data quality [12]. The veracity and accuracy of the data play a crucial role in the effectiveness of big data and predictive analytics applications. Inaccurate or incomplete data can lead to flawed insights and, consequently, misguided decisions. Organizations need to implement robust data governance frameworks to maintain data quality throughout its lifecycle, encompassing data collection, storage, processing, and analysis. This involves establishing clear data quality standards, implementing validation checks, and ensuring data consistency across different sources.

Simultaneously, the models used in predictive analytics must undergo meticulous scrutiny. The success of predictive analytics relies on the ability of these models to accurately represent the underlying patterns in the data. Regular validation and calibration are imperative to ensure that the models remain relevant and effective as data patterns evolve over time [13]. Organizations should also consider the interpretability and explain ability of these models, especially in industries with regulatory or ethical considerations. Transparent models not only enhance trust in the predictions but also facilitate a deeper understanding of the factors influencing the outcomes.

Security Risks with Big Data and Predictive Analytics

Security concerns in the realm of big data and predictive analytics have become paramount as organizations increasingly rely on the consolidation of information from diverse sources into extensive, centralized datasets. The sheer volume and critical nature of this data make safeguarding against potential security risks imperative. One primary concern is the significantly increased attack surfaces inherent in big data architectures, which span across various platforms and networks, creating a multitude of potential points vulnerable to exploitation [14]. Malicious attacks constitute another substantial threat to the security of big data systems. Hackers adept at identifying and exploiting vulnerabilities may target these systems with the intention of either stealing valuable data assets or corrupting the integrity of the analytics models. Such attacks pose a considerable risk given the potential impact on sensitive records and the overall functionality of the data infrastructure.

The importance of robust access controls cannot be overstated in the context of big data security. A proliferation of users with excessively permissive access rights can lead to malicious activities, with unauthorized individuals gaining access to sensitive data. Implementing stringent access controls becomes crucial to mitigate the risk of unauthorized access, data leaks, and potential cyber-attacks.

Encryption emerges as a fundamental security measure to protect big data both at rest and in transit. Inadequate encryption leaves data vulnerable to interception during transmission or unauthorized access when stored. Employing robust encryption protocols is essential to maintaining the confidentiality and integrity of the information contained within large datasets.

The security of big data is further compromised by insecure application programming interfaces (APIs). Poorly secured APIs can serve as entry points for attackers, enabling them to exploit vulnerabilities and gain unauthorized access to the underlying data. Addressing API security concerns is integral to fortifying the overall security posture of big data systems.

Data provenance, encompassing the understanding of the origins and transformations undergone by the data, is a critical aspect of security in the context of predictive analytics. Ensuring the integrity of data for analytical purposes requires a comprehensive understanding of its journey from source to utilization. Provenance issues, if neglected, can introduce uncertainties and compromise the reliability of analytical outcomes [15].

Table 1: Security Controls for Big Data Systems

Control	Description
Network segmentation	Isolate big data systems into separate networks with firewalls
Access controls	Implement role-based access and “least privilege” models
Encryption	Encrypt data in transit and at rest using strong standards
API security	Authenticate API users and authorize access
Data auditing	Log and monitor all access and changes to data
Penetration testing	Ethically hack systems to uncover vulnerabilities

Privacy Risks with Big Data and Predictive Analytics

Privacy concerns loom prominently in the realm of big data, as the aggregation of extensive customer information raises apprehensions regarding potential misuse. The deployment of predictive analytics further intensifies these concerns, as it has the capability to extract sensitive insights from voluminous datasets. One of the primary privacy risks associated with big data is the exposure of personal information through data breaches, which could divulge details such as names, addresses, identification numbers, or browsing histories. The ramifications extend to behavioral profiling, where analytics can categorize individuals based on their behaviors, potentially leading to discriminatory practices or unwarranted predictions [16].

Compounding the privacy challenges is the issue of inadequate consent. Users may find themselves unwittingly subjected to the collection and sharing of their data for purposes they have not expressly permitted. This lack of control over personal information amplifies the vulnerability of individuals within the big data landscape. Furthermore, the secondary usage of personal data poses a significant risk, as information collected for one purpose may be repurposed for entirely different objectives without the knowledge or approval of the data subjects. This unanticipated reuse not only infringes upon individual privacy rights but also underscores the need for stringent data governance measures. The erosion of anonymity emerges as another critical privacy concern in the realm of big data [17]. The combination of multiple datasets has the potential to strip away the veil of anonymity that individuals expect when their information is aggregated. This amalgamation allows for the creation of comprehensive profiles, potentially exposing sensitive details about individuals that were meant to remain private. Consequently, the erosion of anonymity poses a direct threat to the privacy and confidentiality of individuals contributing to large-scale datasets. Moreover, the reliance on big data analytics introduces the risk of flawed inferences, as models may generate inaccurate generalizations based on correlations within the data [18]. The intricate nature of these models, often fueled by machine learning algorithms, can lead to unforeseen biases and inaccuracies in predictions. Such flawed inferences not only compromise the reliability of insights derived from big data but also have real-world implications, potentially perpetuating discriminatory practices or reinforcing existing biases [19].

Table 2: Privacy Controls for Big Data Practices

Control	Description
Consent mechanisms	Seek opt-in consent for data collection and usage
Anonymization	Remove personally identifiable information from datasets
Aggregation	Combine data from individuals into aggregated statistics
Data minimization	Only collect and retain required data
Transparency	Disclose data practices clearly and accessibly
Bias detection	Test models to uncover unfair biases against groups
Audit logging	Record access and usage of personal data

Ethical Considerations for Predictive Analytics

The ethical implications associated with the application of predictive analytics, particularly in the realm of big data analytics, extend beyond concerns of security and privacy. One significant challenge arises from the opacity inherent in the complex nature of machine learning models. The intricate algorithms utilized in predictive analytics often lack transparency, making it challenging to comprehend how specific predictions are generated [20]. This lack of transparency not only hampers the ability to thoroughly scrutinize and identify errors in the models but also poses a barrier to establishing clear accountability for their outcomes. Moreover, the ethical considerations extend to the quality of the data employed in training these predictive models. The efficacy of predictive analytics is heavily contingent upon the quality of the data used during the training phase. If the data is biased, incomplete, or unrepresentative, it can lead to misleading and potentially harmful results. The reliance on such flawed data undermines the integrity and reliability of the predictions, raising ethical concerns about the consequences of acting upon inaccurate or biased information.

An additional ethical challenge arises from the potential reinforcement of bias in predictive models. When these models are trained on historical data reflecting biased human decisions, there is a risk that the same biases will be perpetuated into the future. This perpetuation of bias can contribute to systemic inequalities and hinder efforts to achieve fairness and impartiality in decision-making processes [21]. Discrimination is another critical ethical consideration associated with predictive analytics. Predictions derived from correlations within the data may inadvertently lead to unfair discrimination against certain groups. This discriminatory impact can manifest in various ways, such as in hiring practices, lending decisions, or law enforcement actions. The reliance on predictive analytics raises concerns about reinforcing or exacerbating existing societal disparities and injustices.

The potential for manipulation represents a significant ethical challenge in the context of behavioral targeting through predictive analytics. While the primary purpose of these models is often to enhance user experience or streamline marketing efforts, there is a risk that they may be employed to exploit psychological vulnerabilities for manipulative purposes. This raises ethical concerns regarding the responsible use of predictive analytics and the potential for negative consequences when applied without adequate safeguards. Furthermore, the ethical discourse extends to the concept of human agency. Over-reliance on predictive analytics has the potential to diminish human autonomy and discretion in decision-making processes. When decisions are solely driven by algorithmic predictions, individuals may experience a loss of control over their choices and actions. This erosion of human agency raises fundamental questions about the appropriate balance between automated decision-making and preserving individual autonomy within a society.

Table 3: Ethical Principles for Predictive Analytics

Principle	Description
Explainability	Strive for transparency into data provenance and model design choices
Fairness	Ensure datasets are balanced and unbiased, test for discrimination
Accountability	Assign responsibility for reviewing predictive model inputs, assumptions and outputs

Empowerment	Enable users to understand model outputs and contest unfair inferences
Auditability	Record details of predictions made for each user to enable audits
Human oversight	Keep humans involved in reviewing and evaluating model behaviors

Conclusion

The integration of big data and predictive analytics into organizational processes is a transformative undertaking that offers substantial opportunities and simultaneously introduces complex challenges. The potential value derived from these technologies is considerable, empowering organizations to make data-driven decisions and secure competitive advantages in their respective markets. The fundamental premise lies in the ability to extract meaningful insights from vast datasets, providing a foundation for strategic planning and operational optimization. However, the full realization of these benefits hinges on the effective management of intricate issues surrounding security, privacy, and ethics. Security emerges as a paramount concern in the integration of big data and predictive analytics [22]. The sheer volume and sensitivity of the data involved necessitate robust measures to safeguard against unauthorized access, data breaches, and malicious activities. To mitigate security risks, organizations must implement a comprehensive suite of technical controls. Access management is pivotal, requiring stringent authentication protocols and authorization mechanisms to ensure that only authorized personnel can access and manipulate the data. Encryption serves as a critical layer of defense, safeguarding data both in transit and at rest, thereby preventing unauthorized interception or compromise. Additionally, robust API security measures are imperative to protect the interfaces through which various components of the analytical infrastructure interact. These technical safeguards collectively play a crucial role in securing sensitive information and maintaining the integrity of data analytics processes.

Privacy considerations stand alongside security in significance, as the utilization of big data and predictive analytics often involves the processing of personally identifiable information (PII). Organizations must navigate the intricate landscape of privacy regulations and compliance requirements, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) [23]. Anonymization and pseudonymization techniques are essential tools in preserving privacy, ensuring that individuals cannot be readily identified from the data. Striking a balance between the utility of the data for analytics purposes and the protection of individual privacy rights is a delicate but indispensable task in the integration process [24].

Ethical considerations further complicate the landscape, requiring organizations to establish frameworks that guide responsible and transparent use of data. Questions surrounding bias in algorithms, the fair treatment of different demographic groups, and the potential societal impacts of predictive analytics demand careful attention [25]. Developing and adhering to ethical guidelines ensures that organizations not only comply with legal requirements but also foster trust among stakeholders and the broader community.

Furthermore, the ethical dimensions of big data analytics necessitate careful consideration and management. Clear and comprehensive policies governing data usage consent, anonymization, and retention are imperative to ensure that organizations operate within legal and ethical boundaries. The establishment of ethical principles and oversight mechanisms is essential to prevent potential pitfalls such as discrimination in data analysis [26]. By adhering to a framework of ethical guidelines, organizations can navigate the ethical complexities associated with big data analytics, fostering responsible and socially beneficial practices. In addition, the responsible utilization of big data requires a commitment to transparency and accountability. Organizations must prioritize transparency in their data practices, providing clear communication to stakeholders about how data is collected, processed, and utilized. Concurrently, accountability measures should be established to hold organizations responsible for any misuse of data or violations of privacy and ethical standards. This dual emphasis on transparency and accountability builds trust with stakeholders and the wider public, reinforcing the ethical foundation of big data analytics initiatives. Moreover, the successful integration of big data analytics for social good necessitates ongoing diligence in risk management. Continuous assessment and adaptation of security, privacy, and ethical measures are crucial in the dynamic landscape of data analytics [27]. Organizations must remain vigilant in monitoring emerging threats and evolving regulatory frameworks to ensure compliance and responsiveness to changing conditions. This proactive approach to risk management strengthens the foundation for the responsible and sustainable application of big data analytics in diverse organizational contexts.

The transformative potential of big data and predictive analytics can be harnessed for organizational success and societal benefit, provided that organizations navigate the inherent challenges with diligence and ethical consideration [28]. Technical controls, ethical frameworks, transparency, and accountability collectively form the pillars upon which responsible big data analytics practices can be built [29]. Through a strategic and proactive approach to risk management, organizations can unlock the full potential of big data analytics while upholding the principles of security, privacy, and ethics.

References

[1] J. Béranger, “Chapter 1. From the study of risks to the translation of the ethical issues of Big Data in Health,” *J. Int. Bioethique Ethique Sci.*, vol. 28, no. 3, pp. 15–25, Oct. 2017.

[2] M. Muniswamaiah, T. Agerwala, and C. C. Tappert, “Context-aware query performance optimization for big data analytics in healthcare,” in *2019 IEEE High Performance Extreme Computing Conference (HPEC-2019)*, 2019, pp. 1–7.

[3] A. Li *et al.*, “A geo-spatial database about the eco-environment and its key issues in South Asia,” *Big Earth Data*, vol. 2, no. 3, pp. 298–319, Jul. 2018.

[4] V. Dhar, N. Nilekani, S. Maruwada, and N. Pappu, “Big data as an enabler of primary education,” *Big Data*, vol. 4, no. 3, pp. 137–140, Sep. 2016.

[5] N. Bhatnagar, “Harnessing the power of big data in science,” in *The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2018)*, Cham: Springer International Publishing, 2018, pp. 479–485.

[6] Y. Samuel, J. George, and J. Samuel, “Beyond STEM, how can women engage big data, analytics, robotics and Artificial Intelligence? An exploratory analysis of Confidence and educational factors in the emerging technology waves influencing the role of, and impact upon, women,” *arXiv [cs.CY]*, 26-Mar-2020.

[7] M. Muniswamaiah, T. Agerwala, and C. C. Tappert, “Federated query processing for big data in data science,” in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 6145–6147.

[8] M. Ghasemaghaei, “The role of positive and negative valence factors on the impact of bigness of data on big data analytics usage,” *Int. J. Inf. Manage.*, vol. 50, pp. 395–404, Feb. 2020.

[9] A. Nassar and M. Kamal, “Ethical Dilemmas in AI-Powered Decision-Making: A Deep Dive into Big Data-Driven Ethical Considerations,” *IJRAI*, vol. 11, no. 8, pp. 1–11, 2021.

[10] S. Sioutas, G. Vonitsanos, N. Zacharatos, and C. Zaroliagis, “Scalable and hierarchical distributed data structures for efficient big data management,” in *Algorithmic Aspects of Cloud Computing*, Cham: Springer International Publishing, 2020, pp. 122–160.

[11] L. Yuqi, “Analysis of algorithmic infringement risk in the background of big data,” *Criminal Justice Science & Governance*, vol. 1, no. 1, pp. 88–97, 2020.

[12] S. Salloum, J. Z. Huang, Y. He, and X. Chen, “An asymptotic ensemble learning framework for big data analysis,” *IEEE Access*, vol. 7, pp. 3675–3693, 2019.

[13] M. D. M. Islam, M. D. A. Razzaque, M. M. Hassan, W. N. Ismail, and B. Song, “Mobile cloud-based big healthcare data processing in smart cities,” *IEEE Access*, vol. 5, pp. 11887–11899, 2017.

[14] S. Belfkih, A. Ait Lahcen, F. Z. Benjelloun, and A. Oussous, “NoSQL databases for big data,” *Int. J. Big Data Intell.*, vol. 4, no. 3, p. 171, 2017.

[15] U. Bhuvan, “NoSQL databases and big data strategies,” in *Big Data Strategies for Agile Business*, Auerbach Publications, 2017, pp. 283–309.

[16] A. Nassar and M. Kamal, “Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies,” *Intelligence and Machine Learning …*, 2021.

[17] S. Fosso Wamba, S. Akter, A. Edwards, G. Chopin, and D. Gnanzou, “How ‘big data’ can make big impact: Findings from a systematic review and a longitudinal case study,” *Int. J. Prod. Econ.*, vol. 165, pp. 234–246, Jul. 2015.

[18] M. Muniswamaiah, T. Agerwala, and C. Tappert, “Big data in cloud computing review and opportunities,” *arXiv preprint arXiv:1912.10821*, 2019.

[19] D. B. Ventura, “Exploring the Perceptions, Influences, and Sociodemographic Determinants of Sustainable Fashion among Consumers in Colombia,” *IJRAI*, vol. 5, no. 3, pp. 1–14, Mar. 2015.

[20] D. Bholat, “Big Data and central banks,” *Big Data Soc.*, vol. 2, no. 1, p. 205395171557946, May 2015.

[21] C. L. Philip Chen and C.-Y. Zhang, “Data-intensive applications, challenges, techniques and technologies: A survey on Big Data,” *Inf. Sci.* , vol. 275, pp. 314–347, Aug. 2014.

[22] R. Kirkpatrick, “Big data for development,” *Big Data*, vol. 1, no. 1, pp. 3–4, Mar. 2013.

[23] M. Muniswamaiah, T. Agerwala, and C. C. Tappert, "Approximate query processing for big data in heterogeneous databases," in *2020 IEEE International Conference on Big Data (Big Data)*, 2020, pp. 5765–5767.

[24] X. W. Chen and X. Lin, "Big data deep learning: challenges and perspectives," *IEEE access*, 2014.

[25] H. Chen, R. H. L. Chiang, and V. C. Storey, "Business Intelligence and Analytics: From Big Data to Big Impact," *Miss. Q.*, vol. 36, no. 4, pp. 1165–1188, 2012.

[26] J. E. Johnson, "Big data+ big analytics= big opportunity: big data is dominating the strategy discussion for many financial executives. As these market dynamics continue to evolve …," *Financial Executive*, 2012.

[27] A. Mavragani and G. Ochoa, "The internet and the anti-vaccine movement: Tracking the 2017 EU measles outbreak," *Big Data Cogn. Comput.*, vol. 2, no. 1, p. 2, Jan. 2018.

[28] A. Kankanhalli, J. Hahn, S. Tan, and G. Gao, "Big data and analytics in healthcare: Introduction to the special section," *Inf. Syst. Front.*, vol. 18, no. 2, pp. 233–235, Apr. 2016.

[29] D. B. Ventura, "Promoting Sustainability in the Fashion Industry: An Exploratory Study of Fashion Sharing in Colombia," *ijsa*, vol. 1, no. 7, pp. 1–12, Jul. 2016.