Penerbit Akademia Baru

Journal of Advanced Research Design

Journal homepage:
https://akademiabaru.com/submit/index.php/ard
ISSN: 2289-7984

Enhancing Big Data Governance Practices: Addressing Security, Privacy and Ethical Challenges

Yunusa Adamu Bena[1,2], Roliana Ibrahim[1], Jamilah Mahmood[1], Farkhana Muchtar[1,*], Chan Weng Howe[1], Muhammad Zafran Muhammad Zaly Shah[1], Zuriahati Mohd Yunos[1], Salmah Fattah[2]

[1] Faculty of Computing, Universiti Teknologi Malaysia, Skudai, 81310 Johor Bahru, Johor, Malaysia
[2] Faculty of Computing and Informatics, Universiti Malaysia Sabah, 88400 Kota Kinabalu, Sabah, Malaysia

ARTICLE INFO

Article history:
Received 7 February 2025
Received in revised form 21 March 2025
Accepted 15 July 2025
Available online 11 August 2025

Keywords:
Big data; big data governance; security; privacy; ethical concerns; maturity assessment model

ABSTRACT

The exponential growth of data from diverse sources has amplified the challenges of managing security, privacy and ethical concerns in big data governance. Organizations face significant risks related to data breaches, regulatory compliance and ethical dilemmas, necessitating robust governance frameworks. This study examines the state of BDG practices in data-driven organizations, focusing specifically on security, privacy and ethical concerns. Through a systematic literature review of 53 peer-reviewed articles published between 2019 and 2024, the study identifies critical gaps and opportunities in current governance practices. The findings reveal that while BDG practices enhance data security, ensure compliance and foster ethical accountability organizations struggle with fragmented frameworks, insufficient scalability and a lack of unified strategies for addressing interconnected challenges. To bridge these gaps, this study proposes the Security, Privacy and Ethical Concerns Maturity Assessment Model (SPEC MAM), which evaluates governance maturity across four dimensions: Security, Privacy, Ethical Concerns and Integrated Concerns. The model categorizes maturity into four progressive stages: Foundational, Policy Development, Integrated Practices and Proactive, providing organizations with a structured approach to assess and enhance governance maturity. While the model offers a systematic framework for addressing BDG challenges, its real-world application and scalability remain areas for further exploration. This study contributes to academia and practice by advancing BDG research and equipping organizations with actionable strategies to address security, privacy and ethical concerns in an increasingly complex data landscape.

1. Introduction

In the digital age, big data has emerged as a cornerstone for innovation and growth across a wide range of sectors. However, the rapid proliferation and replication of datasets have introduced significant challenges, particularly in the areas of security, privacy and ethics. According to Ghafoor *et al.,* [1], these challenges not only threaten the integrity and confidentiality of data but also raise complex ethical questions regarding data usage, privacy rights and the responsibilities of those who

* *Corresponding author*
E-mail address: farkhana@utm.my

https://doi.org/10.37934/ard.142.1.159176

govern organizational data. As a result, conventional data governance frameworks have increasingly proven inadequate in addressing these multifaceted issues [2-5], largely due to their rigidity and inability to adapt swiftly to modern technological advancements [3,4]. Kusi-Sarpong *et al.,* [6] asserts that modern organizations require a robust data governance framework that centralizes governance processes while ensuring the effective usability, consistency and security of data assets. However, Sun *et al.,* [7] highlight the lack of effective methods and approaches for improving the security aspects of big data governance as a major barrier to its adoption by contemporary organizations. Similarly, Elwan *et al.,* [3] and Trom *et al.,* [8] points to irregularities in data integrity as a critical challenge, preventing organizations from adequately addressing security, privacy and ethical concerns in big data governance.

Some scholars, such as Yebenes *et al.,* [9] and Zorilla *et al.,* [10], argue that one of the underlying causes of these challenges is the lack of comprehensive data literacy programs within organizations, which would provide regular training to employees on data security, privacy and ethical responsibilities. Moreover, the absence of clear methodological approaches to guide organizations in managing governance policies, regulatory compliance and data protection further exacerbates these issues [2]. As noted by Kaginalkar *et al.,* [11], existing big data governance frameworks tend to focus primarily on the integration of data sources, often overlooking critical issues related to security and privacy [7].

This study seeks to address the pressing challenges of security, privacy and ethical concerns identified in the literature as critical issues within big data governance practices. To achieve this, the study conducted a focused literature review exploring the multidimensional challenges and complexities associated with these three components. The review synthesizes the current state of research on how organizations are managing security risks, ensuring data privacy and upholding ethical principles in an increasingly data-driven world. By highlighting gaps and opportunities in existing governance frameworks, the study provides a comprehensive understanding of how addressing security, privacy and ethical concerns can lead to more resilient and sustainable big data governance practices. This study has defined three (3) research questions (RQ) that align with its overall aim. The formulated research questions are as follows:

i. RQ1. What is the existing security, privacy and ethical challenges of big data governance?
ii. RQ2. What are the current approaches for addressing the security, privacy and ethical challenges of big data governance?
iii. RQ3. How can a model be developed to assess and mitigate the security, privacy and ethical challenges in big data governance program?

The objectives of this study are as follows to:

i. Explore and identify the existing challenges in big data governance programs, with a focus on security, privacy and ethical concerns as highlighted in the literature
ii. Examine the current approaches used to address these identified challenges
iii. Develop a model that can evaluate and assess the maturity stage of an organization's security, privacy and ethical challenges on big data governance program and highlight areas for improvement.

1.1 Background of Study

This section provides an overview of big data governance on security, privacy and ethical challenges, drawing from previous studies to summarize their core definitions, characteristics and relevance to modern organizational challenges. Big data governance, which focuses on the management and control of vast, complex data environments, has become an essential component for organizations seeking to ensure data security, privacy and ethical compliance. As data volumes continue to grow exponentially, traditional governance frameworks are proving inadequate to handle the unique challenges posed by big data, such as scalability, real-time data processing and diverse data sources. This has led to the need for more dynamic, adaptable governance models that can respond to the ever-evolving landscape of big data. Therefore, this study situates itself at the intersection of these pressing challenges, aiming to provide a structured approach to evaluating and addressing security, privacy and ethical concerns within big data governance. By exploring the complexities of these components and their interplay, this research seeks to contribute to the development of sustainable and resilient governance practices that enable organizations to effectively manage their data assets while fostering trust and accountability in a data-driven society.

2. Literature Review

2.1 Big Data

Big data refers to extremely large and complex datasets generated from heterogenous sources [1-4,12,13]. It is often described by the "4Vs": volume (i.e., the sheer amount of data generated); velocity (the speed at which data is produced and processed); variety (the different types of data, including structured, semi-structured and unstructured data); and veracity (i.e., the uncertainty or trustworthiness of the data) [9,11]. Big data is generated from a heterogenous sources, of which include social media platforms, sensors, mobile devices, transactions and web interactions, resulting in an ever-increasing flow of information [11,12]. The rise of big data presents organizations with both opportunities and challenges [13,14]. On one hand, big data provides the potential to uncover valuable insights, predict trends and enhance decision-making processes by analysing large datasets [17-19]. On the other hand, managing such vast and diverse data requires sophisticated governance frameworks to ensure data quality, security and privacy [15,16].

2.2 Big Data Governance

Big data governance is an evolving concept that attracts many researchers. However, more effort is required from this domain area [2,11]. Although, most of the identified definitions of big data governance from the previous literature were drawn from Data Management Body of Knowledge (DAMA-DMBOK) guide, which defines data governance as “the exercise of authority and control (planning, monitoring and enforcement) over the management of data assets DAMA [17].” This definition provides a foundational understanding of governance, focusing on authority, control and the structured management of data. However, as the scope and complexity of big data have grown [16,18], scholars have expanded this definition to suit specific contexts and applications.

For instance, Rahmadian *et al.,* [15] describes big data governance as a multifaceted process that involves organizational stakeholders, methodologies, protocols, tools and technologies, all working together to enable organizations to harness their data as a valuable digital asset. This view emphasizes the collaborative and interdisciplinary nature of big data governance, highlighting the need for coordination across various departments and roles within an organization. In contrast,

Ghafoor *et al.,* [1] and Kaginalkar *et al.,* [11] offer a more procedural approach, defining big data governance as a set of processes, policies and practices designed to ensure that data is managed efficiently, securely and in compliance with regulatory standards. This definition underscores the importance of security and compliance, key concerns in the management of vast and diverse data sets.

These varied perspectives reflect the complexity of big data governance, which must address not only technical challenges but also organizational [19], regulatory and ethical concerns. As data becomes increasingly central to decision-making and innovation [20], the role of big data governance in ensuring data integrity, security and ethical use becomes even more critical [21].

2.3 Impact of Big Data Governance on Organizations

The impact of big data governance programs on modern organizations cannot be overstated [1]. While many organizations struggle to fully implement such program due to concerns over security, privacy and ethical issues [21], those that do benefit significantly from the robust protection and control that effective governance provides [22]. A well-structured big data governance program establishes clear security protocols, safeguarding data against unauthorized access and breaches [23]. By defining who can access data, under what conditions and implementing mechanisms to control how data is protected organizations are better equipped to maintain data integrity and confidentiality [19].

In addition to preventing security incidents, comprehensive big data governance program incorporates encryption practices and enable regular security audits, ensuring that data remains protected against evolving cyber threats [7]. These practices help organizations not only comply with regulatory standards but also build trust with stakeholders by demonstrating their commitment to data security [20,24]. Moreover, big data governance plays a crucial role in safeguarding privacy [25]. By establishing policies and practices that govern how sensitive information is collected, processed, stored and shared organizations can ensure compliance with privacy regulations and mitigate the risk of data misuse or violations [26]. This not only protects individuals' rights but also enhances organizational reputation and trustworthiness in an era where data privacy is increasingly a focal concern for both consumers and regulators [24-26]. In this way, big data governance is essential for balancing the benefits of data-driven innovation with the need for security, privacy and ethical integrity in the digital landscape.

3. Methodology

3.1 Review Protocol

This study conducted a comprehensive review of Big Data Governance, with a particular focus on critical aspects such as security, privacy and ethical concerns in data governance practices. A thorough analysis was performed on 53 scholarly articles published between 2019 and 2024, sourced from five reputable academic databases: Web of Science, ScienceDirect, Emerald, Springer and Google Scholar. 53 studies were selected from the domain of Big Data Governance, emphasizing the emerging challenges and strategies related to data security, privacy protections and ethical considerations in data management. These studies highlight the pressing need for robust frameworks and approaches to mitigate risks associated with data breaches, ensure compliance with privacy regulations and address ethical issues such as bias and transparency in data governance. These studies were selected for their relevance in addressing the interdependencies between security, privacy and ethical challenges in big data governance. This approach underscores our research

commitment to a holistic understanding of big data governance, integrating technical resilience with ethical accountability. Furthermore, this study applied specific inclusion and exclusion criteria in selecting the articles for review, as detailed in Table 1.

Table 1
Articles selection criteria

Criteria	Inclusion	Exclusion
Language	Studies in English language	Other languages
Availability	Full-text studies	Uncompleted studies
Publication year	Between 2019-2024	Earlier than 2019
Articles	Only journals	Conference & Book chapters

3.2 Studies Selection Criteria

The article selection for this study was guided by four key criteria to ensure the relevance and quality of the included research. Only studies published in English were included, while those in other languages were excluded. Full-text studies were selected for review and incomplete or unavailable studies were excluded. The review focused on studies published between 2019 and 2024 to ensure that the findings reflect the latest trends and emerging challenges in big data governance, particularly concerning security, privacy and ethical concerns, with studies published prior to 2019 excluded. To maintain a focus on high-quality research, only peer-reviewed journal papers were included, while conference papers and book chapters were excluded.

The article selection for this study was guided by four key criteria to ensure the relevance and quality of the included studies. First, language was a primary filter, with only studies published in English being included, while those in other languages were excluded. Second, availability was considered, with only full-text studies being selected for review, excluding incomplete studies. Third, the publication year was restricted to works published between 2019 and 2024, ensuring that the findings are current and reflect the latest trends in big data governance. Studies published prior to 2019 were excluded. Lastly, the type of articles was limited to peer-reviewed journal papers, with conference papers and book chapters being excluded to maintain a focus on high-quality, well-vetted research.

4. Research Questions' Results

This section presents the findings based on the research questions outlined in this study, each of which addresses critical aspects of big data governance in solving organizational challenges. The research questions were designed to explore key issues such as security, privacy and ethical challenges within big data governance frameworks, as well as the effectiveness of current approaches in mitigating these issues.

To ensure clarity and structure of the findings, the results have been categorized into the four fundamental components of big data governance: people, process, data and technology. These categories help to organize the insights derived from the literature, ensuring a comprehensive understanding of how each component interacts with the challenges and solutions identified. The following sections provide detailed discussions on the outcomes for each research question, offering a structured response to the:

i. Existing security, privacy and ethical challenges of big data governance
ii. Current approaches used to address these challenges

iii. Proposed Security, Privacy and Ethical Concerns Maturity Assessment Model (SPEC MAM).

4.1 The Existing Security, Privacy and Ethical Challenges of Big Data Governance (RQ1)

The findings related to the existing security, privacy and ethical challenges in big data governance are outlined in the following table. These challenges represent key issues that modern organizations face when managing vast amounts of data. The analysis reveals vulnerabilities related to data breaches, unauthorized access, regulatory compliance and ethical data usage. Additionally, concerns about the protection of sensitive information and the ethical implications of data-driven decision-making are highlighted. These challenges, if left unaddressed, can significantly undermine the effectiveness of big data governance programs. Table 2 presents a comprehensive overview of these challenges, categorized according to the core components of big data governance: people, process, data and technology. This classification enables a clearer understanding of how each aspect of governance contributes to these challenges, providing a foundation for exploring potential solutions in subsequent sections.

Table 2
Security, privacy and ethical challenges of big data governance

Challenge(s)	Challenge(s)	Description(s)	Reference(s)
People	Privacy invasion	Reveal of personal information from anonymized data, can lead to privacy invasions.	[12,27,28]
	Data ownership	The ambiguities about who owns data can lead to ethical dilemmas and conflicting rights and responsibilities.	[21,22,29,30]
	Bias and discrimination	Decisions can become perpetuated when there is Discrimination among the stakeholders.	
	Ethical use of data	Identifying what constitutes ethical use of big data, in contexts like human behaviour prediction and manipulation.	
	Data literacy program	Lack of data literacy program can lead to security, privacy and ethical challenges across the organization.	[1,20,31,32]
Process	Informed consent	To obtain genuine consent is challenging in big data contexts due to unforeseen processes.	[11,29,33-35]
	Transparency	The complexity of big data algorithms makes it difficult for stakeholders to understand how data is being used.	
Data	Data breaches	The volume of big data increases the vulnerability to breaches, risking exposure of sensitive information.	[19,36-40]
	Data accuracy	Poor data quality or outdated data can lead to inaccurate analyses and reliability of decisions on data.	
	Regulatory compliance	Adhering to evolving regulatory frameworks like GDPR or HIPAA can be challenging.	
Technology	Surveillance and monitoring	Using modern technologies to gain unauthorized access about individual freedoms and privacy.	[18,41-43]

The analysis of the identified challenges in big data governance reveals several critical issues across the fundamental components: people, process, data and technology.

i. People-related challenges: include privacy invasion, data ownership ambiguities, bias and discrimination, ethical use of data and the lack of data literacy programs. Privacy invasion occurs when anonymized data reveals personal information, while data ownership conflicts lead to ethical dilemmas regarding rights and responsibilities. Bias and discrimination can

arise in decision-making processes, impacting the fairness of big data usage among stakeholders. Additionally, the ethical use of data, particularly in contexts such as behaviour prediction and manipulation, remains a contentious issue. A significant challenge is the lack of data literacy programs within organizations, which leads to security, privacy and ethical violations, demonstrating the need for continuous education on data governance practices.

ii. Process-related challenges: focus on the difficulties of obtaining informed consent and maintaining transparency in big data environments. Gaining genuine informed consent is challenging due to the unforeseen nature of data processes and the complexity of data collection. Furthermore, the lack of transparency around how big data algorithm's function makes it difficult for stakeholders to fully understand how their data is being used, increasing concerns about privacy and misuse.

iii. Data-related challenges: dominated by concerns over data breaches, data accuracy and regulatory compliance. The vast volume of data increases the vulnerability to breaches, exposing sensitive information to unauthorized parties. Data accuracy is another critical issue, as poor data quality can lead to inaccurate analysis and unreliable decision-making. Compliance with evolving regulations, such as the GDPR and HIPAA, adds another layer of complexity, as organizations must continually adapt to meet new legal requirements.

iv. Technology-related challenges: centre around surveillance and monitoring, where modern technologies are used to gain unauthorized access to personal data, raising concerns about privacy and the potential for misuse of information. The rise of surveillance technologies poses a significant threat to individual freedoms and privacy, further complicating the landscape of big data governance.

In conclusion, these challenges highlight the multifaceted nature of big data governance issues, spanning across people, processes, data and technology. Addressing these concerns requires a comprehensive governance framework that not only ensures compliance and security but also fosters transparency, ethical use and stakeholder engagement.

4.2 The Existing Approaches for Addressing the Security, Privacy and Ethical Challenges of Big Data Governance Program (RQ2)

Following the identification of the key challenges in big data governance on security, privacy and ethical concerns, this section presents the identified existing approaches for addressing these challenges. Table 3 provides a comprehensive overview of the approaches identified from previous studies, highlighting the methods employed to enhance data governance practices and mitigate the risks associated with big data. The analysis of existing approaches for addressing the security, privacy and ethical challenges in big data governance programs reveals several key strategies across four main components (i.e., people, process, data and technology).

i. People-focused approaches: This approach emphasize the importance of involving stakeholders from various departments [19], assigning clear roles and responsibilities within data governance teams [44] and establishing data literacy programs [22,31]. These measures are essential for fostering a culture of accountability and ensuring that all employees are equipped with the knowledge and skills necessary to handle data responsibly [8,38].

ii. Process-related approaches: The approach include the development of holistic data governance frameworks that integrate organizational processes and foster cross-departmental synergy [45,46]. Engaging relevant departments to work collaboratively

enhances accountability in data management [6,7], while enforcing data quality standards ensures that data remains reliable and fit for decision-making purposes [26,47].

iii. Data-centred approaches: This approach focuses on compliance with international standards and data privacy regulations, such as ISO 8000-61 for data quality, ISO/IEC 38505 for data governance, ISO/IEC 27001 for information security, ISO 19600 for compliance management and GDPR [21,48,49]. These standards provide structured guidelines for managing data quality, security and regulatory compliance [18,37]. Additionally, setting internal data quality standards and establishing data lifecycle management practices help ensure data integrity and protect sensitive information [39,50].

iv. Technology-driven approaches: Leverage advanced tools and methodologies to enhance data governance. For instance, the use of fuzzy logic helps evaluate data governance activities, while talent management systems (TMS) support skills alignment in data governance roles.

Table 3
Approaches for mitigating the security, privacy and ethical challenges of big data governance

Component(s)	Approach(es)	References
People	By involving stakeholders across each department. Assigning clear roles and responsibilities to data governance teams. Establishing data literacy program.	[8,14,19,27,36,38,51]
Process	By developing a holistic DG framework or models that integrate organizational processes. Engaging relevant departments to operate in synergy and enforce accountability measures for data management. By enforcing data quality standards.	[6,7,12, 23,52]
Data	Ensure compliance with ISO standards (e.g., ISO 8000-61 for data quality management, ISO/IEC 38505 for governance of data, ISO/IEC 27001 for information security management and ISO 19600 for compliance management system). Compliance with data privacy regulations (e.g., GDPR). By setting data quality standards. Establishing data lifecycle management.	[18,37,39,50,53]
Technology	Using fuzzy logic approach to evaluate the data governance activities. Deploying talent management system (TMS). Deploying modern data governance tools e.g., data catalogue, data lineage, Collibra and Ataccana ONE. Deploying data visualization tools (e.g., BI Dashboards) to monitor the data governance processes. By implementing data classification schemas.	[19,21,29,33,36,37,54-57]

The deployment of modern data governance tools, such as data catalogues, data lineage tools, Collibra and Ataccana ONE, along with data visualization tools like BI dashboards, enables real-time monitoring of governance processes. Implementing data classification schemas further enhances data organization and security [19,21,37].

4.3 The Proposed Maturity Assessment Model (RQ3)

This question explores how a maturity assessment model can be developed to evaluate, assess and mitigate the challenges of security, privacy and ethical concerns within the context of big data governance programs. The question also underscores the critical need for organizations to establish frameworks that not only diagnose existing challenges of BDG but also provide actionable strategies to enhance governance practices. The results presented in this section reflect the practical

application of the proposed model in identifying gaps and implementing solutions to mitigate security, privacy and ethical risks. By focusing on these interconnected domains, the findings aim to provide organizations with a roadmap for achieving resilience and accountability in their data governance practices. Therefore, the detailed analysis of the model's performance, effectiveness, adaptability and potential for fostering sustainable governance in complex data environments is also highlighted.

4.3.1 Overview of the proposed model

This The In today's interconnected and data-driven world, the challenges of ensuring security, privacy and ethical stewardship in data governance are more significant than ever. Organizations face an urgent need to adopt comprehensive and sustainable practices that safeguard sensitive data, maintain compliance with evolving regulations and uphold ethical standards in their operations. The literature highlights the increasing demand for frameworks and models that address these critical aspects, emphasizing their importance in enabling organizational resilience and growth.

As identified by this study, integrating security, privacy and ethical considerations into a cohesive governance strategy presents inherent challenges but remains a foundational step in fostering sustainable practices. With heightened awareness of these challenges organizations are increasingly seeking methods to evaluate and enhance their maturity in addressing these domains. Therefore, this study has introduced the security, privacy and ethical concerns Maturity assessment model (SPEC MAM), with a structured and innovative approach designed to assess the maturity level of organizations in managing these challenges. The SPEC MAM provides a practical framework for evaluating current practices, identifying gaps and guiding towards an improved DG practice. By addressing challenges in a unified manner, this model aims to guide organizations toward achieving effective and sustainable DG practices in an era defined by complex data environment.

4.3.2 Model development

The model is designed to support organizations in addressing the unique challenges of safeguarding sensitive data, maintaining privacy and upholding ethical standards within their data governance practices. This model offers a structured framework for evaluating the maturity level of an organization's initiatives in managing security, privacy and ethical concerns. It identifies the current state of maturity while highlighting critical gaps and areas for improvement, enabling organizations to make informed decisions to advance their practices. Whether an organization is at the beginning stages or has already implemented robust measures, the model serves as a strategic tool to guide continuous improvement and ensure comprehensive data governance practices.

The MAM uniquely integrates the four critical dimensions of Security, Privacy, Ethical Concerns and Integrated Concerns, offering a holistic approach to addressing modern DG governance challenges. By consolidating these dimensions, the model empowers organizations to navigate the complexities of today's data environment and develop resilient strategies for handling the organizational data. Through an interactive evaluation process organizations can objectively assess their maturity level, identify critical weaknesses and implement targeted enhancements to strengthen their DG governance practices. The MAM provides actionable insights and clear guidance for interpreting assessment outcomes and planning progressive steps to achieve excellence in managing security, privacy and ethical challenges. This innovative model equips organizations with the tools needed to align their practices with global standards, ensuring accountability, compliance and ethical stewardship in an increasingly interconnected and data-driven world.

4.3.3 Model dimensions

The proposed model is developed upon four critical dimensions: Security, Privacy, Ethical Concerns and Integrated Concerns. These dimensions serve as the foundational pillars for evaluating and enhancing an organization's governance practices, particularly in addressing the challenges associated with safeguarding sensitive data, ensuring compliance and upholding ethical standards. Each dimension represents a unique but interconnected aspect of DG governance, collectively supporting organizations in establishing effective and sustainable DG practices. By addressing these dimensions holistically organizations can systematically evaluate their maturity, identify gaps and implement improvements that align with modern governance requirements.

Consolidating the focus on security, privacy and ethical challenges across these dimensions is vital for achieving a resilient and accountable governance framework. Figure 1 presents the 4 dimensions that form the core building blocks of the proposed model. The detailed description of each dimension, emphasizing their contributions to advancing organizational maturity in managing security, privacy and ethical concerns are discussed as follows:

i. Security: The Security dimension evaluates the organization's ability to protect its data assets and systems from threats and unauthorized access. This dimension focuses on the implementation of risk identification and mitigation strategies, secure access controls, encryption techniques and incident response mechanisms. It also examines the maturity level of regular security audits, compliance with security standards and employee training on cybersecurity practices. Additionally, this dimension assesses the deployment of advanced tools and technologies for threat detection and monitoring, ensuring the organization's resilience against potential data breaches and vulnerabilities in its data governance practices.
ii. Privacy: The Privacy dimension focuses on the organization's approach to safeguarding personal and sensitive information generated by intelligent systems. It evaluates the maturity of privacy policies and mechanisms such as anonymization, pseudonymization and secure data sharing. This dimension also assesses compliance with local and international privacy regulations (e.g., GDPR, HIPAA) and the organization's ability to address data subject rights, including access and erasure requests. Furthermore, it evaluates how organizations ensure privacy-by-design principles and conduct regular updates to privacy policies to keep pace with evolving regulations. Training programs on privacy practices are also a key component of this dimension.
iii. Ethical Concerns: The Ethical Concerns dimension evaluates the organization's commitment to addressing ethical issues related to data governance. This dimension examines the presence of frameworks for bias detection and mitigation, guidelines for ethical AI usage and mechanisms to ensure transparency and accountability in data practices. It also evaluates the organization's efforts to engage stakeholders in ethical reviews and their ability to conduct ethical impact assessments. Training programs for employees on ethical data handling and policies for preventing discriminatory outcomes are additional aspects of this dimension, ensuring responsible and fair usage of data generated by intelligent systems.
iv. Integrated Concerns: The Integrated Concerns dimension assesses the organization's ability to address security, privacy and ethical challenges in a unified and holistic manner. This dimension evaluates cross-functional collaboration and alignment of governance practices with organizational and regulatory policies. It also examines the maturity level of integrated risk management frameworks, automated governance workflows and scalable solutions for data governance. Furthermore, this dimension assesses the organization's ability to

continuously improve and adapt governance practices to evolving data-driven environments, ensuring that security, privacy and ethical considerations are seamlessly interwoven into its overall data governance strategy.

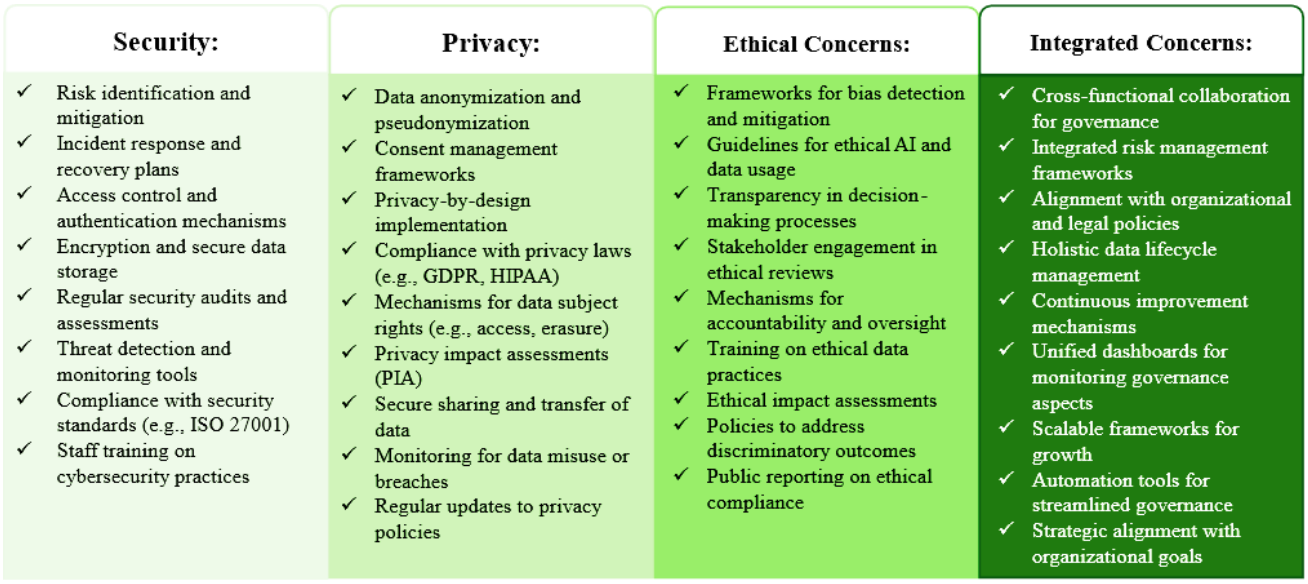

Fig. 1. The proposed model' dimensions

4.3.4 Maturity stages in the proposed model

The stages of the proposed maturity assessment model provide a structured framework for evaluating an organization's progression in managing critical aspects of data governance. These stages are designed to help organizations identify their current maturity level, uncover challenges in addressing security, privacy and ethical concerns and prioritize strategic actions for improvement. Unlike conventional maturity models, which often rely on generalized benchmarks, the stages in this model are specifically tailored to the four dimensions: Security, Privacy, Ethical Concerns and Integrated Concerns.

Similarly, the model is divided into four progressive stages: Foundational awareness, Policy development, Integrated practices and Proactive practices. Each stage represents a significant milestone in the organization's journey toward achieving robust and sustainable practices for addressing security, privacy and ethical challenges. As organizations progress through these stages, they can expect to realize greater operational efficiency, enhanced compliance and improved stakeholder trust.

Figure 2 illustrates the progression through these stages, offering a clear path for interpreting assessment results. The stages provide the necessary context for understanding the organization's maturity level and identifying actionable areas for improvement. This model developed 12 survey questions as input for assessing an organization's maturity level. Out of these questions 3 are on security, 3 on privacy, 4 on ethical concerns and 2 on integrated concerns. Moreover, the number responses from 1- 4 from questions on every dimension represents the stages of maturity of an organization's data governance practices on security, privacy, ethical and integrated concerns. The criteria for assessing the maturity stages are categorized into two approaches: 1. One directional response and 2. Mixed responses.

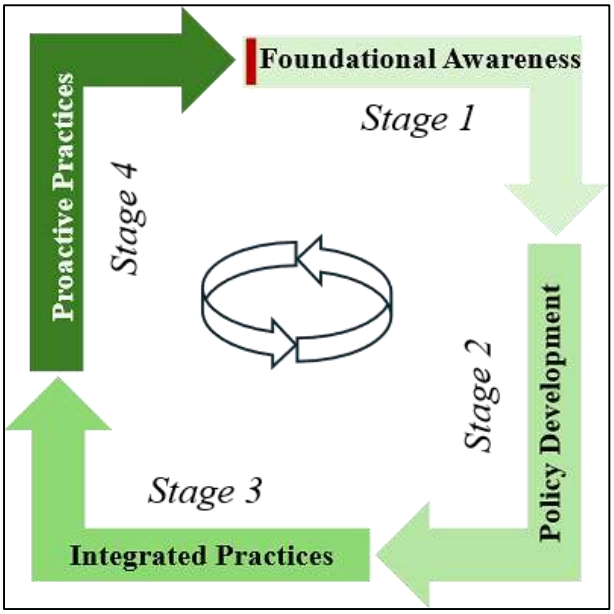

Fig. 2. Stages of maturity in the proposed model

4.3.4.1 One-directional responses

i. Foundational Awareness Stage: If an organization's responses to all 12 survey questions fall under "Option 4", the organization is classified in the "Foundational Awareness Stage". This indicates that the organization has no formal security, privacy, ethical and integrated concerns' mechanisms in place, but has plans for future improvements. Efforts are minimal and frameworks, policies and processes are in the conceptual stage.
ii. Policy Development Stage: If an organization's responses to all 12 survey questions fall under "Option 3", the organization is classified in the "Policy Development Stage". At this stage, the organization is in the planning phase. Initial steps are being taken to conceptualize security, privacy, ethical and integrated concerns' mechanisms processes.
iii. Integrated Practices Stage: If an organization's responses to all 12 survey questions fall under "Option 2", the organization is classified in the Integrated Practices Stage. Security frameworks, privacy and ethical processes are partially functional and the organization is making progress in operationalizing its mechanisms practices.
iv. Proactive Practices Stage: If an organization's responses to all 12 survey questions fall under "Option *1*", the organization is classified in the "*Proactive Stage*. This represents the highest level of maturity in terms of security, privacy and addressing the ethical concerns and comprehensive and fully operational frameworks, policies and processes are implemented effectively.

4.3.4.2 Mixed-responses approach

In the case of mixed-responses approach, for instance if an organization's responses multiple options, additional options and guidelines determining the scores has been developed. In this regards we categorized the approach into two (2):

i. Numerical weight approach
ii. Weighted percentage approach.

Below are the guidelines for assessment:

i. Numerical weight approach. Assign numerical weights:

- Option 1 (proactive stage): 4 points;
- Option 2 (integrated practices stage): 3 points;
- Option 3 (policy development stage): 2 points;
- Option 4 (foundational stage): 1 point.
- Calculate the total score: Multiply the response frequency for each option by its corresponding weight and sum up the total weighted score across all 12 survey questions. Example, if an organization answers:
  - 4 questions as Option 1
  - 5 questions as Option 2
  - 2 questions as Option 3
  - 1 question as Option 4
- The total score is calculated as:
  (4×4) +(5×3) +(2×2) +(1×1) =16+15+4+1=36(4 \times 4) + (5 \times 3) + (2 \times 2) + (1 \times 1) = 16 + 15 + 4 + 1 = 36.
- Determine the average score: Divide the total score by the number of survey questions (12 in this case):

$$\text{Average Score} = \frac{\text{Total Score}}{\text{Number of Questiond}} = \frac{36}{12} = 3.0 \quad (1)$$

- Map the average score to maturity stages: Use the following mapping: 3.5-4.0 (proactive stage), 2.5-3.49 (integrated practices stage), 1.5-2.49 (policy development stage) and 1.0-1.49 (foundational stage). Therefore, in this example, the average score is 3.0, which places the organization in the "integrated practices stage" of maturity in terms of security, privacy and ethical concerns.

ii. Weighted percentage approach. Here are the guidelines for determining the maturity using this approach. For example, if an organization responded to the 12 survey questions as follows:

- Option 1 (proactive stage): 3 questions
- Option 2 (integrated practices stage): 4 questions
- Option 3 (policy development stage): 4 questions
- Option 4 (foundational stage): 1 question
- Step 1: Calculate the percentage of responses for each option. Divide the number of responses for each option by the total number of questions (12) and multiply by 100 to calculate percentages:
  - $\text{Option } 1 = \frac{3}{12} \times 100 = 25\%$
  - $\text{Option } 2 = \frac{4}{12} \times 100 = 33.33\%$
  - $\text{Option } 3 = \frac{4}{12} \times 100 = 33.33\%$
  - $\text{Option } 4 = \frac{1}{12} \times 100 = 8.33\%$
- Step 2: Assign weights to each option. Use the following weights for the maturity stages:
  - Option 1 (proactive stage): 4 points
  - Option 2 (integrated practices stage): 3 points
  - Option 3 (policy development stage): 2 points

- Option 4 (foundational stage): 1 point
- Step 3: Multiply each percentage by its weight. For each option, multiply the percentage by its corresponding weight:
- Option 1: 25%×4=1.025\% \times 4 = 1.0
- Option 2: 33.33%×3=1.033.33\% \times 3 = 1.0
- Option 3: 33.33%×2=0.6733.33\% \times 2 = 0.67
- Option 4: 8.33%×1=0.0838.33\% \times 1 = 0.083
- Step 4: Sum up the weighted values. Add the weighted values to calculate the overall weighted score:

  1.0+1.0+0.67+0.083=2.7531.0 + 1.0 + 0.67 + 0.083 = 2.753
- Step 5: Map the weighted score to a maturity stage. Use the following mapping:
- 3.5-4.0: Proactive stage
- 2.5-3.49: Integrated practices stage
- 1.5-2.49: Policy development stage
- 1.0-1.49: Foundational stage

In this example, the organization's overall weighted score is 2.753, which places it in the "Integrated practices stage" of maturity.

4.3.5 Impact and applicability of the proposed model

The Security, Privacy and Ethical Concerns Maturity Assessment Model (SPEC MAM) is developed as a versatile and comprehensive tool for evaluating and enhancing BDG governance practices in organizations. The SPEC MAM also offer a structured framework to assess organizational maturity and provide actionable pathways for improvement. The proposed is developed to enable organizations to:

i. Strengthen their DG practices by identifying critical gaps across the dimensions of security, privacy, ethical concerns and integrated concerns, the model also empowers organizations to fortify their governance frameworks.
ii. It enhances risk management in facilitating a proactive approach to mitigating risks associated with data breaches, privacy violations and ethical dilemmas, ensuring greater resilience.
iii. Achieve compliance and trust by assisting organizations to align their practices with global standards and regulatory requirements, fostering trust among stakeholders and improving transparency.
iv. It fosters continuous improvement through its progressive maturity stages; the SPEC MAM drives organizations to move systematically from foundational practices to proactive governance excellence.

5. Discussion

This study addresses the critical challenges of security, privacy and ethical concerns within the domain of Big Data Governance (BDG), focusing on organizations generating data from diverse and complex sources. The proposed Security, Privacy and Ethical Concerns Maturity Assessment Model (SPEC MAM) provides a structured framework for assessing governance maturity across four dimensions: Security, Privacy, Ethical Concerns and Integrated Concerns. The model categorizes organizations into four progressive stages "Foundational", "Policy Development", "Integrated

Practices" and "Proactive" to reflect their journey toward governance excellence. The findings from the literature review highlight that while organizations increasingly recognize the importance of BDG, many faces persistent issues such as fragmented frameworks, limited scalability and inadequate mechanisms for addressing security, privacy and ethical concerns. These challenges are exacerbated by the rapid growth of data and the evolving regulatory environment. The SPEC MAM addresses these gaps by offering a practical and actionable framework to evaluate governance practices, identify deficiencies and prioritize improvements.

The discussion underscores the importance of aligning governance practices with global regulatory standards, fostering ethical accountability and implementing robust security measures to mitigate risks. The proposed model not only emphasizes a holistic approach to governance but also enables organizations to enhance operational efficiency, strengthen stakeholder trust and achieve sustainable growth in a data-driven environment. While the SPEC MAM provides a valuable tool for organizations, its practical implementation in real-world contexts and scalability across various industries warrant further exploration. Future studies should validate the model through empirical research, applying it to diverse organizational settings to assess its adaptability and effectiveness. By addressing these gaps, the SPEC MAM advances both academic discourse and practical applications, equipping organizations to navigate the complexities of modern data landscapes effectively.

6. Limitations and Future Directions

This study provides a robust framework through the Security, Privacy and Ethical Concerns maturity assessment model to address critical challenges in BDG. However, certain limitations warrant consideration. First, the model's development is primarily based on insights from a literature review and its practical implementation has yet to be validated through empirical studies in real-world organizational settings. Second, while the model offers a structured approach to governance, its adaptability to diverse industries and varying organizational scales remains untested.

Future research should focus on validating the SPEC MAM in diverse organizational contexts to assess its effectiveness and adaptability. Further studies should also investigate how the SPEC MAM can be customized to address sector-specific challenges, ensuring broader applicability and scalability across industries. These directions will contribute to refining the model and advancing the discourse on BDG practices in an increasingly complex data environment.

Acknowledgement

This research was supported by the Universiti Teknologi Malaysia (UTM) Encouragement Research Grant under project reference number PY/2024/01535.

References

[1] Ghafoor, Laib and Fatima Tahir. *Data Governance in the Era of Big Data: Best Practices and Strategies*. No. 10941. EasyChair, 2023.

[2] Marelli, Luca, Giuseppe Testa and Ine Van Hoyweghen. "Big Tech platforms in health research: Re-purposing big data governance in light of the General Data Protection Regulation's research exemption." *Big Data & Society* 8, no. 1 (2021): 20539517211018783. https://doi.org/10.1177/20539517211018783

[3] Elwan, Esraa A., Mohamed Elkawkagy and Arabi Keshk. "Enhancing Fine Grained Technique for Maintaining Data Privacy." *Journal of Advanced Research in Computing and Applications* 10, no. 1 (2018): 1-6.

[4] Hao, Lei, Khoo Terh Jing, Zhang Ruirui, Ha Chin Yee, Shi Yangle and Chen Siyao. "Application of big data in the prevention of work-related crimes in early-stage construction engineering." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 32, no. 2 (2023): 457-474. https://doi.org/10.37934/araset.32.2.457474

[5] Varghese, Jijo and P. Tamil Selvan. "A Novel Clustering and Matrix Based Computation for Big Data Dimensionality Reduction and Classification." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 32, no. 1 (2023): 238-251. https://doi.org/10.37934/araset.32.1.238251

[6] Kusi-Sarpong, Simonov, Ifeyinwa Juliet Orji, Himanshu Gupta and Martin Kunc. "Risks associated with the implementation of big data analytics in sustainable supply chains." *Omega* 105 (2021): 102502. https://doi.org/10.1016/j.omega.2021.102502

[7] Sun, Liyuan, Hongyun Zhang and Chao Fang. "Data security governance in the era of big data: status, challenges and prospects." *Data Science and Management* 2 (2021): 41-44. https://doi.org/10.1016/j.dsm.2021.06.001

[8] Trom, Lomso and Johannes Cronje. "Analysis of data governance implications on big data." In *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 1*, pp. 645-654. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-12388-8_45

[9] Yebenes, Juan and Marta Zorrilla. "Towards a data governance framework for third generation platforms." *Procedia Computer Science* 151 (2019): 614-621. https://doi.org/10.1016/j.procs.2019.04.082

[10] Zorrilla Pantaleón, Marta E. and Juan Rafael Yébenes Serrano. "A reference framework for the implementation of data governance systems for industry 4.0." *Computer Standard & Interfaces* 81 (2021): 103595 https://doi.org/10.1016/j.csi.2021.103595

[11] Kaginalkar, Akshara, Shamita Kumar, Prashant Gargava, Neelesh Kharkar and Dev Niyogi. "SmartAirQ: A big data governance framework for urban air quality management in smart cities." *Frontiers in Environmental Science* 10 (2022): 785129. https://doi.org/10.3389/fenvs.2022.785129

[12] Zaki, Ummu Hani'Hair, Izyan Izzati Kamsani, Ahmad Firdaus Ahmad Fadzil, Zainura Idrus and Eser Kandogan. "Big data: Issues and challenges in clustering data visualization." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 51, no. 1 (2025): 150-159. https://doi.org/10.37934/araset.51.1.150159

[13] Bhojan, Rajendran and Saravanan Venkataraman. "Big data analysis on network intrusion detection using high performance deep neural networks." *Journal of Advanced Research in Applied Sciences and Engineering Technology* (2024): 167-176. https://doi.org/10.37934/araset.55.1.167176

[14] Nisar, Qasim Ali, Nadia Nasir, Samia Jamshed, Shumaila Naz, Mubashar Ali and Shahzad Ali. "Big data management and environmental performance: role of big data decision-making capabilities and decision-making quality." *Journal of Enterprise Information Management* 34, no. 4 (2021): 1061-1096. https://doi.org/10.1108/JEIM-04-2020-0137

[15] Rahmadian, Eko, Daniel Feitosa and Yulia Virantina. "Digital twins, big data governance and sustainable tourism." *Ethics and Information Technology* 25, no. 4 (2023): 61. https://doi.org/10.1007/s10676-023-09730-w

[16] Brous, Paul, Marijn Janssen and Rutger Krans. "Data governance as success factor for data science." In *Conference on e-Business, e-Services and e-Society*, pp. 431-442. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-44999-5_36

[17] Mosley, Mark, Michael Brackett, Susan Earley. *The DAMA Guide to The Data Management Body of Knowledge (DAMA-DMBOK Guide)*. DAMA International, 2009.

[18] Basukie, Jessica, Yichuan Wang and Shuyang Li. "Corrigendum to "Big data governance and algorithmic management in sharing economy platforms: A case of ridesharing in emerging markets" technological forecasting & social change 161 (2020) 120310." *Technological Forecasting and Social Change* 163 (2021): 120423. https://doi.org/10.1016/j.techfore.2020.120423

[19] Ahmadi, Sadra, Mohammad Mahdi Tavana, Sajjad Shokouhyar and Mina Dortaj. "A new fuzzy approach for managing data governance implementation relevant activities." *The TQM Journal* 34, no. 5 (2022): 979-1012. https://doi.org/10.1108/TQM-01-2021-0015

[20] Gupta, Rahul and Sukritindra Soni. "Developing effective big data strategies and governance frameworks: principles, tools, challenges and best practices." *International Journal of Responsible Artificial Intelligence* 10, no. 8 (2020): 10-19.

[21] McMahon, Aisling, Alena Buyx and Barbara Prainsack. "Big data governance needs more collective responsibility: the role of harm mitigation in the governance of data use in medicine and beyond." *Medical Law Review* 28, no. 1 (2020): 155-182. https://doi.org/10.1093/medlaw/fwz016

[22] Kaushik, Shweta. "Big Data Issues and Challenges." In *Big Data Applications for Improving Library Services*, p. 1-21. IGI Global, 2021. https://doi.org/10.4018/978-1-7998-3049-8.ch001

[23] Feng, Yunzhong and Xiaohua Feng. "Smart data analysis and data governance." In *Proceedings of the 5th International Conference on Computer Science and Application Engineering*, p. 1-5. 2021. https://doi.org/10.1145/3487075.3487112

[24] Rasheed, Mansoor Ahmad, Hafiz Zeeshan Ahmad, Hafiz Abdullah Tanweer, Hudabia Murtaza, Mannan Ahmad Rasheed and Mishaal Ahmed. "Use of big data governance in several corporate sectors." *VFAST Transactions on Software Engineering* 9, no. 4 (2021): 92-101. https://doi.org/10.21015/vtse.v9i4.729
[25] Rhahla, Mouna, Sahar Allegue and Takoua Abdellatif. "Guidelines for GDPR compliance in Big Data systems." *Journal of Information Security and Applications* 61 (2021): 102896. https://doi.org/10.1016/j.jisa.2021.102896
[26] Yang, Longzhi, Jie Li, Noe Elisa, Tom Prickett and Fei Chao. "Towards big data governance in cybersecurity." *Data-Enabled Discovery and Applications* 3, no. 1 (2019): 10. https://doi.org/10.1007/s41688-019-0034-9
[27] Micheli, Marina, Marisa Ponti, Max Craglia and Anna Berti Suman. "Emerging models of data governance in the age of datafication." *Big Data & Society* 7, no. 2 (2020): 2053951720948087. https://doi.org/10.1177/2053951720948087
[28] Zihao, Deng, Khoo Terh Jing, Ha Chin Yee, Shi Yangle, Zhou Zilin, Chen Siyao, Sun Hui and Li Yao. "The nexus between construction contract risk assessment and big data in China." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 33, no. 1 (2023): 441-448. https://doi.org/10.37934/araset.33.1.441448
[29] Rasheed, Mansoor Ahmad, Hafiz Zeeshan Ahmad, Hafiz Abdullah Tanweer, Hudabia Murtaza, Mannan Ahmad Rasheed and Mishaal Ahmed. "Use of big data governance in several corporate sectors." *VFAST Transactions on Software Engineering* 9, no. 4 (2021): 92-101. https://doi.org/10.21015/vtse.v9i4.729
[30] Zhahir, Amirul Asyraf, Siti Munirah Mohd, Mohd Ilias M. Shuhud, Bahari Idrus, Hishamuddin Zainuddin, Nurhidaya Mohd Jan and Mohamed Ridza Wahiddin. "Enhancing quantum information processing–SU (2) Operator model development for three-qubit quantum systems entanglement classification." *International Journal of Computational Thinking and Data Science* 3, no. 1 (2024): 1-19. https://doi.org/10.37934/ctds.3.1.119
[31] Rasheed, Mansoor Ahmad, Hafiz Zeeshan Ahmad, Hafiz Abdullah Tanweer, Hudabia Murtaza, Mannan Ahmad Rasheed and Mishaal Ahmed. "Use of big data governance in several corporate sectors." *VFAST Transactions on Software Engineering* 9, no. 4 (2021): 92-101. https://doi.org/10.21015/vtse.v9i4.729
[32] Ferretti, Agata. "Ethics and governance of big data in health research and digital health applications." PhD diss., ETH Zurich, 2021.
[33] Al-Ruithe, Majid, Elhadj Benkhelifa and Khawar Hameed. "A systematic literature review of data governance and cloud data governance." *Personal and Ubiquitous Computing* 23 (2019): 839-859. https://doi.org/10.1007/s00779-017-1104-3
[34] Yousfi, Siham, Dalila Chiadmi and Maryem Rhanoui. "Smart big data framework for insight discovery." *Journal of King Saud University-Computer and Information Sciences* 34, no. 10 (2022): 9777-9792. https://doi.org/10.1016/j.jksuci.2021.12.009
[35] Singh, Dalbir. "Towards data privacy and security framework in big data governance." *International Journal of Software Engineering and Computer Systems* 6, no. 1 (2020): 41-51. https://doi.org/10.15282/ijsecs.6.1.2020.5.0068
[36] Yukhno, Alexander. "Digital transformation: Exploring big data governance in public administration." *Public Organization Review* 24, no. 1 (2024): 335-349. https://doi.org/10.1007/s11115-022-00694-x
[37] Surbakti, Feliks P. Sejahtera, Wei Wang, Marta Indulska and Shazia Sadiq. "Factors influencing effective use of big data: A research framework." *Information & Management* 57, no. 1 (2020): 103146. https://doi.org/10.1016/j.im.2019.02.001
[38] Knapton, Ken. "Exploring Mid-Market Strategies for Big Data Governance." *Adv. Artif. Intell. Mach. Learn.* 3, no. 1 (2023): 816-838. https://doi.org/10.54364/AAIML.2023.1151
[39] Cengiz, Nezerith, Siti M. Kabanda, Tonya M. Esterhuizen and Keymanthri Moodley. "Exploring perspectives of research ethics committee members on the governance of big data in sub-Saharan Africa." *South African Journal of Science* 119, no. 5-6 (2023): 1-9. https://doi.org/10.17159/sajs.2023/14905
[40] Alkhalaf, Abeer, Bassel Alkhatib and Safwan Ghanem. "SQL injection attack detection using machine learning techniques." In *International Conference on Advanced Computing and Intelligent Engineering*, pp. 145-156. Singapore: Springer Nature Singapore, 2022. https://doi.org/10.1007/978-981-99-5015-7_13
[41] Liu, Xuanzhe, Sam Xun Sun and Gang Huang. "Decentralized services computing paradigm for blockchain-based data governance: Programmability, interoperability and intelligence." *IEEE Transactions on Services Computing* 13, no. 2 (2019): 343-355.
[42] Kun, Wang, Liu Tong and Xie Xiaodan. "Application of big data technology in scientific research data management of military enterprises." *Procedia Computer Science* 147 (2019): 556-561. https://doi.org/10.1016/j.procs.2019.01.221

[43] Kurniawan, Dwitama Heryadi, Yova Ruldeviyani, Mohammad Rizky Adrian, Sutia Handayani and M. Rizki Pohan. "Data governance maturity assessment: a case study in it bureau of audit board." In *2019 International Conference on Information Management and Technology (ICIMTech)* 1, p. 629-634. IEEE, 2019. https://doi.org/10.1109/ICIMTech.2019.8843742
[44] Mateen, Arab ul, Qasim Ali Nisar, Samia Jamshed, Sumaira Rehman and Muhammad Ali. "HRM effectiveness as an outcome of big data: The role of big data–driven HR practices and electronic HRM." *Journal of the Knowledge Economy* (2024): 1-35. https://doi.org/10.1007/s13132-024-02216-0
[45] Obatolu, R. "A holistic framework for complex big data governance." PhD diss., University of East London, 2022.
[46] Aderemi, Samuel Omololu. "Exploring the impact of big data on data governance." PhD diss., Walden University, 2024.
[47] Liu, Zhao-ge, Xiang-yang Li and Xiao-han Zhu. "Scenario modeling for government big data governance decision-making: Chinese experience with public safety services." *Information & Management* 59, no. 3 (2022): 103622. https://doi.org/10.1016/j.im.2022.103622
[48] Verdugo, Javier and Moisés Rodríguez. "Assessing data cybersecurity using ISO/IEC 25012." *Software Quality Journal* 28, no. 3 (2020): 965-985. https://doi.org/10.1007/s11219-019-09494-x
[49] Christodoulou, Eleni and Kalypso Iordanou. "Democracy under attack: challenges of addressing ethical issues of AI and big data for more democratic digital media and societies." *Frontiers in Political Science* 3 (2021): 682945. https://doi.org/10.3389/fpos.2021.682945
[50] Zhang, Hongbin and Hanchi Zhang. "Discussion on the Role of Big Data in Improving Public Sector Governance." *Journal of Innovation and Development* 2, no. 2 (2023): 133-136. https://doi.org/10.54097/jid.v2i2.6405
[51] Basukie, Jessica, Yichuan Wang and Shuyang Li. "Big data governance and algorithmic management in sharing economy platforms: A case of ridesharing in emerging markets." *Technological Forecasting and Social Change* 161 (2020): 120310. https://doi.org/10.1016/j.techfore.2020.120310
[52] Janssen, Marijn, Paul Brous, Elsa Estevez, Luis S. Barbosa and Tomasz Janowski. "Data governance: Organizing data for trustworthy artificial intelligence." *Government information quarterly* 37, no. 3 (2020): 101493. https://doi.org/10.1016/j.giq.2020.101493
[53] Zhang, Qingqiang, Xinbo Sun and Mingchao Zhang. "Data matters: A strategic action framework for data governance." *Information & Management* 59, no. 4 (2022): 103642. https://doi.org/10.1016/j.im.2022.103642
[54] Okuyucu, Aras and Nilay Yavuz. "Big data maturity models for the public sector: a review of state and organizational level models." *Transforming Government: People, Process and Policy* 14, no. 4 (2020): 681-699. https://doi.org/10.1108/TG-09-2019-0085
[55] OvalEdge. *Why AI Governance Should Begin During Design, Not Deployment*. Linked in 2024.
[56] Varshney, Sharad and Kieron Allen. *Implementing Data Governance: How to Develop a Strategy, Determine a Value Proposition and Build a Business Case*. OvalEdge p. 1–32, 2020.
[57] Ferretti, Agata, Marcello Ienca, Minerva Rivas Velarde, Samia Hurst and Effy Vayena. "The challenges of big data for research ethics committees: A qualitative Swiss study." *Journal of Empirical Research on Human Research Ethics* 17, no. 1-2 (2022): 129-143. https://doi.org/10.1177/15562646211053538