Online-Journals.org

iTDAF IETI Transactions on
Data Analysis and Forecasting

iTDAF | eISSN: 2959-0442 | Vol. 2 No. 1 (2024) | OPEN ACCESS

https://doi.org/10.3991/itdaf.v2i1.46779

PAPER

Cybersecurity and Efficacity of Open Data Platforms

Besart Hyseni(✉), Lejla Abazi Bexheti

Faculty of Contemporary Sciences and Technologies, South East European University, Tetovo, North Macedonia

bh29738@seeu.edu.mk

ABSTRACT

Cybersecurity is critical for protecting open data. Transparency and innovation are facilitated by open data platforms; however, concerns about cybersecurity and privacy persist. This study examines the role of cybersecurity in public institutions in the Republic of Kosovo to determine methods of safeguarding data integrity. The main aim of this study was to examine the role of cybersecurity in securing open data in public organizations in the Republic of Kosovo. The study aimed to identify optimal cybersecurity practices in the context of open data and provide a comprehensive overview of the implementation of cybersecurity measures. This study employed a structured and methodical approach to assess cybersecurity and the effectiveness of open data platforms in public organizations in the Republic of Kosovo. Results: The study provides an overview of the status of open data platforms in the Republic of Kosovo and highlights the importance of cybersecurity, data privacy, and data integrity. Despite the stated concerns, such as enhancing security measures and increasing user knowledge, it is evident that public institutions have made significant progress in securing and enhancing their open data platforms. It is suggested that institutions in the Republic of Kosovo continue to invest in cybersecurity, promote privacy protection measures, and focus on enhancing the quality of open data to develop in this sector. Furthermore, collaboration and coordination across institutions and government agencies are required to enhance the efficiency and effectiveness of these platforms.

KEYWORDS

cybersecurity of open data platforms, efficacy, data protection and quality, Republic of Kosovo public institutions

1 INTRODUCTION

Cybersecurity is crucial for ensuring the integrity, reliability, and accessibility of open data platforms in light of growing cyber threat sophistication and an uptick in data breaches [21, 39, 46]. The convergence of the increasing importance of open data platforms and the evolving cyber threats requires a comprehensive analysis [21]. The emergence of these platforms has transformed data sharing, encouraging openness, creativity, and public participation [46]. However, its global expansion has

Hyseni, B., Bexheti, L.A. (2024). Cybersecurity and Efficacity of Open Data Platforms. *IETI Transactions on Data Analysis and Forecasting (iTDAF)*, 2(1), pp. 4–22. https://doi.org/10.3991/itdaf.v2i1.46779

Article submitted 2023-11-15. Revision uploaded 2024-01-07. Final acceptance 2024-01-10.

raised concerns about cybersecurity, data protection, and privacy [46]. Open data platforms, distinguished by their accessibility and unrestricted data sharing, have become indispensable in various industries. They enable governments to publicly disclose crucial information, companies to innovate, and academic institutions to disseminate knowledge [25]. Given the increasing frequency and sophistication of cyber threats, which have made data breaches and ransomware attacks common and highly alarming [13], cybersecurity plays a crucial role in securing data on these platforms.

The study delves into the complex relationship between open data and cybersecurity, exploring key concepts and themes. It underscores the significance of cybersecurity in preserving and protecting open data platforms through case studies and the identification of best practices. The study provides insights into formulating strategies and implementing cybersecurity measures to secure data-sharing initiatives while maintaining stakeholder trust and participation.

The importance of open data extends to the corporate sector, where it serves as a significant resource for market analysis and product creation while also raising ethical concerns and data privacy issues [10]. The interaction between open data and cybersecurity is a source of concern for governments, corporations, and academic institutions in the digital age [9–10]. Understanding this ever-changing ecosystem is critical for reaping the benefits of open data while maintaining data integrity and security [10]. The primary research question explores how cybersecurity, acting as a protective shield, impacts the effectiveness and utility of open data platforms, particularly within the governmental institutions of the Republic of Kosovo. The research outlines interconnected goals, such as a meticulous examination of cybersecurity's fundamental role, a critical assessment of the benefits and challenges of open data initiatives, and a case study analysis involving relevant institutions in Kosovo under ASHI [the Information Society Agency of the Republic of Kosovo]. The ultimate objective is to gain a comprehensive understanding of historical practices, challenges, and opportunities in managing open data platforms, focusing on cybersecurity, data quality, user engagement, and data sharing within the public sector of the Republic of Kosovo.

2 LITERATURE REVIEW

The Role of Cybersecurity in open data platforms – Data interchange has revolutionary potential for governments, corporations, and academics, aided by open data platforms that provide transparent access to large datasets. Strong cybersecurity measures are required to protect platform integrity and security [11]. With the increasing significance of platforms, heightened cybersecurity measures are crucial in the governmental, corporate, and academic sectors. Cybersecurity is the primary line of defense against potential breaches, protecting sensitive data and preventing unauthorized access, manipulation, and compromise of critical information [12]. Breach incidents have disastrous implications, weakening public trust and jeopardizing data-driven decision-making [12]. A comprehensive cybersecurity strategy, which includes access control and encryption, is necessary to guarantee authorized data access and safeguard data during transmission and storage [13]. Open data platforms with robust cybersecurity frameworks enable quick reaction capabilities, detecting and responding to incidents as soon as they occur [13]. Recent incidents highlight the critical relevance of cybersecurity, with government initiatives imposing strict controls and security evaluations [17]. Data.gov in the

United States promotes cybersecurity through continuous monitoring and encryption [13]. The private sector employs comprehensive cybersecurity measures for market analysis and innovation, relying on open data. Cybersecurity is crucial on open data platforms for ensuring data integrity, building user trust, and enhancing platform efficiency. Data anonymization and permission methods are critical for safeguarding individual privacy and ensuring ethical data usage, and they warrant attention [14]. Comprehensive cybersecurity strategies are required to reap the benefits of open data platforms, such as openness and innovation. As the digital world grows, the crucial relevance of cybersecurity in open data extends to governments, corporations, and academics [14].

Benefits and challenges of open data platforms – Transparency, innovation, and public involvement are facilitated by open data platforms in the public and corporate sectors. Despite undeniable benefits, there are problems that require solutions for optimal operation. Transparency is increased, revealing government, commercial, and academic activities, while privacy and legal issues arise. Innovation thrives, enabling large corporations and researchers, yet variations in data quality raise concerns about dependability. Although public involvement is thriving, uneven access limits inclusivity. Data-driven decision-making enhances choices while complicating relevance. The economic potential of open data is enormous, but challenges related to sustainability and standards require constant attention. Balancing openness and security is critical for preserving the benefits of open data [15–18].

Case studies and best practices – Success on open data platforms requires the efficient adoption of best practices and case study findings [16]. Practical experience analysis is critical for providing valuable insights on efforts to enhance open data platforms. For data security, case studies emphasize the crucial need for safe access restrictions, strong user authentication, and frequent security assessments [16]. Successful open data initiatives with robust cybersecurity measures safeguard proprietary data and consumers in the commercial sector, emphasizing continuous threat assessment and proactive incident response [21]. Collaboration and data sharing encourage innovation, emphasizing the catalytic role of cybersecurity in data governance [4, 16]. For enterprises and governments, practical insights enhance the productivity and security of open data platforms.

Public sector and government initiatives – Governments and public entities are leading the way in adopting open data platforms, acknowledging their potential for transparency, citizen participation, and innovation [17]. Global public-sector initiatives have significantly boosted the utilization of open data in governance by establishing standards and best practices [17]. These efforts altered the government-citizen relationship by simplifying the process for individuals to analyze operations and actively engage in policymaking [17]. Platforms for open data promote the social contract by encouraging trust, cooperation, and innovation [18]. However, challenges such as data quality, consistency, and sustainability persist, requiring resources and quality control systems. Government policies utilize anonymisation techniques and robust privacy protection measures to strike a balance between the advantages of open data and individual privacy. Best practices from government initiatives have a significant impact on the effectiveness of open data platforms [17–18].

Data privacy and ethical considerations – Cybersecurity risks on open data platforms create data privacy concerns, requiring a delicate balance between transparency and individual protection [17, 18, 20]. This challenge is exemplified by the New York City Open Data program, which underscores the crucial importance of robust anonymisation techniques such as differential privacy and k-anonymity [17, 18, 20]. Transparency, fair data gathering, and informed consent are all ethical considerations in open data, promoting trust and accountability. The integration of AI and machine learning into open data platforms complicates data privacy issues, requiring adaptive methods [19–20]. For future endeavors, user-centered design, data governance, education [22], and ongoing monitoring are advocated, highlighting the critical importance of data privacy and ethics in open data platforms [21–24].

Open data in the private sector – The rise of open data in the business sector provides strategic benefits, influencing competition, social responsibility, and societal impact. Market research, product development, business intelligence, cost savings, corporate social responsibility (CSR), open data marketplaces, collaborations, data-driven marketing, sustainability, data quality, privacy, security, and governance are some of the key benefits [30–35]. Despite the hurdles, implementing ethical norms enables effective utilization of open data [36–43]. As new technologies emerge, open data platforms integrate AI, blockchain, IoT, and edge computing. Future developments will focus on data-sharing ecosystems, integration, personalized experiences, enhanced security, and privacy [38–41]. However, issues such as data privacy, quality, standardization, governance, and security continue to affect the open data ecosystem [41–48].

3 METHODOLOGY

The methodology of this study provides a structured and systematic approach to investigating cybersecurity and the effectiveness of open data platforms in public institutions in the Republic of Kosovo.

The study aimed to gain a comprehensive understanding of past practices, challenges, and opportunities in managing open data platforms, with a specific focus on previous cybersecurity measures, data quality, user engagement, and data sharing in the public sector in the Republic of Kosovo.

Like many other countries, the Republic of Kosovo recognizes the potential of open data platforms to enhance transparency, accountability, and public access to information. Open data initiatives are crucial for promoting data-driven decision-making, fostering innovation, and driving economic and social development. However, the successful implementation of these initiatives has largely relied on previous cybersecurity measures to protect data integrity and prevent previous cyber threats.

The methodology has played a pivotal role in achieving the objectives of this study. The study employed an integrated approach to research methods, combining qualitative methods such as a literature review with quantitative methods through a survey conducted with officials in public institutions in the Republic of Kosovo.

The main objectives of the research were as follows:

- To assess the state of cybersecurity policies and practices in public institutions in the Republic of Kosovo, with a particular emphasis on open data platforms.
- To evaluate the effectiveness of data encryption methods in securing open data platforms.
- To examine access control mechanisms and user models for open data platforms, including the usage of multi-factor authentication.
- To assess data quality control measures and data security practices in place on open data platforms.

- To investigate how user feedback is collected and utilized to enhance the functionality and content of open data platforms.
- To analyze data privacy measures and data ownership policies governing open data platforms.
- To explore collaborations with other government departments and external organizations to enhance the content and functionality of open data platforms.
- To measure the impact and effectiveness of open data initiatives and provide examples of their benefits to the public and decision-makers.
- To assess the challenges that public institutions face in maintaining secure and effective open data platforms and to identify opportunities for improvement.
- To examine the plans and priorities of public institutions for improving their cybersecurity and the effectiveness of their open data platforms.

The study focused on evaluating the state of open data platforms in public institutions within the Republic of Kosovo and aimed to deliver actionable recommendations for enhancing cybersecurity and efficiency. Using a robust stratified random sampling technique, the study involved 60 employees and experts from various public institutions, ensuring a representative sample.

A structured questionnaire was designed to collect data on cybersecurity and platform efficiency, covering aspects such as past policies, data encryption, access control, usage, data quality, user feedback, collaboration, impact assessment, data management, and future plans. Qualitative methods, such as document content analysis and interviews, were combined with quantitative analysis using statistical tests like descriptive statistics, correlation analysis, and regression analysis for a comprehensive assessment.

The study made important contributions by providing insights into previous cybersecurity procedures, overall platform efficiency, and the influence of open data efforts on decision-making and the public. It is a resource for public organizations to identify areas for development and enhance data security. Policymakers may use the findings to make more informed decisions, allocate resources, and formulate policies, promoting openness and accountability in the public sector of the Republic of Kosovo's. Despite its thorough approach, the study has limitations, including potential selection bias due to the representativeness of the sample and reliance on self-reported data, which is prone to inaccuracies. Given the specific setting of Kosovo, findings may not be generalizable outside the country and may be influenced by insufficient record-keeping and institutional responses. Furthermore, as technology and cybersecurity landscapes evolve, certain conclusions may become obsolete. The framework of the research, which includes questions and hypotheses, provides a comprehensive structure for evaluating cybersecurity and efficiency on open data platforms within Kosovo's governmental institutions. The predicted outcomes serve as a foundation, but the actual findings, as they emerge during the research process, will provide the most accurate representation. Finally, the study aimed to provide authentic insights and recommendations for enhancing cybersecurity and improving the overall effectiveness of open data platforms in the Republic of Kosovo.

4 RESULTS

The study aims to enhance the understanding of cybersecurity policies and practices as well as the effectiveness of encryption and access control methods on open data platforms in the Republic of Kosovo. We examine whether public institutions have established cybersecurity policies, deployed encryption and access control measures, improved data quality, and incorporated user input for changes using the assumptions provided below.

Hypothesis 1: Public institutions in the Republic of Kosovo have established cybersecurity policies and practices for open data platforms.

The Table 1 below presents the results of the study on the identification and classification of data in public institutions in the Republic of Kosovo. The results indicate that 33.3% of respondents have mentioned data identification and classification as a key aspect of their cybersecurity policies, while 72.2% have confirmed the practical use of these measures. This finding suggests that institutions are actively engaged in identifying and classifying data through various means to enhance cybersecurity. At the same time, the results show that a smaller percentage of respondents, approximately 25.6%, have mentioned data security as part of their cybersecurity policies, and 55.6% have confirmed the use of this measure. This confirms that data security is an important aspect of cybersecurity policies in public institutions in the Republic of Kosovo.

Table 1. Kosovo's open cybersecurity

$H1 Frequencies				
		Responses		Percent of Cases
		N	Percent	
H1[a]	Identification and classification of data	39	33.3%	72.2%
	Data security	30	25.6%	55.6%
	Auditing and monitoring	9	7.7%	16.7%
	Personnel training	24	20.5%	44.4%
	Protection against security breaches	15	12.8%	27.8%
Total		117	100.0%	216.7%

Note: [a]Dichotomy group tabulated at value 1.

However, the overall percentage of monitored and audited data and personnel training is lower. Only 7.7% of respondents mentioned security auditing and monitoring, while 16.7% confirmed the use of this practice. Similarly, only 20.5% of respondents mentioned personnel training as an aspect of their cybersecurity policies, and 44.4% confirmed the use of this measure. In summary, these results offer an initial insight into cybersecurity practices in public institutions in the Republic of Kosovo. While some users have confirmed the implementation of certain cybersecurity policy measures, there is still a need to increase awareness and attention to other aspects of cybersecurity in these institutions. This implies that, despite research suggesting the incorporation of cybersecurity policies, there are challenges in improving their implementation and awareness in this field. Based on these results, we can conclude that the hypothesis is confirmed. Public institutions in the Republic of Kosovo have established cybersecurity policies and practices for open data platforms. The results indicate that these institutions have mentioned data identification, classification, and security measures as part of their cybersecurity practices, confirming their practical application.

Hypothesis 2: Data transmitted and stored on open data platforms in the Republic of Kosovo is adequately encrypted.

The Table 2 below presents information on various aspects of data security and privacy on open data platforms in the Republic of Kosovo. From the results, it appears that 43.1% of respondents have confirmed the use of data encryption, while 26.9% have mentioned the use of privacy policies, and 18.5% have reported the use of access restrictions. These figures indicate that some security and privacy practices are present in open data platforms on the Republic of Kosovo, with a certain percentage of institutions utilizing encryption and privacy policies.

Table 2. Kosovo data encryption

What Quality Control Measures are Applied Regarding Data Encryption?				
		Responses		Percent of Cases
		N	Percent	
H2[a]	Privacy policies	32	26.9%	62.7%
	Access Restrictions	22	18.5%	43.1%
	Data encryption	22	18.5%	43.1%
	Acceptance of open data	12	10.1%	23.5%
	Data flow	9	7.6%	17.6%
	Security auditing and monitoring	12	10.1%	23.5%
	Compliance with legal regulations	10	8.4%	19.6%
Total		119	100.0%	233.3%

Note: [a]Dichotomy group tabulated at value 1.

Based on the presented data, we can conclude that there is a basis to support the hypothesis that the data transmitted and stored on open data platforms in the Republic of Kosovo is adequately encrypted. From the percentage of encryption usage, it appears that a significant number of institutions have implemented this measure to ensure the security of open data. However, it is important to thoroughly assess other aspects of data security and privacy to make a more comprehensive evaluation of the situation in the Republic of Kosovo.

Hypothesis 3: Access control measures, including multi-factor authentication (MFA), are utilized to regulate access to open data platforms in the Republic of Kosovo.

The Table 3 below contains statistics on access control mechanisms on open data platforms in the Republic of Kosovo. According to the findings, a significant number of respondents have reported using various access control methods on these sites. For example, 32.5% of respondents stated that rigorous access restrictions were used to limit user settings and permissions, while 20.0% stated that MFA was used to safeguard data access. This demonstrates an understanding of the importance of access constraints in open data systems.

Table 3. Kosovo MFA access

How Does Your Institution Control Access to Open Data on the Platform?		Responses		Percent of Cases
		N	Percent	
H3[a]	Using advanced access and authorization systems for users.	12	15.0%	20.7%
	Implementing multi-factor authentication (MFA) to secure data access.	16	20.0%	27.6%
	Using digital certificates for user identification.	9	11.3%	15.5%
	Monitoring user activity on the platform to detect potential breaches.	17	21.3%	29.3%
	Employing strict access policies to control user settings and permissions.	26	32.5%	44.8%
Total		80	100.0%	137.9%

Note: [a]Dichotomy group tabulated at value 1.

We can confirm the hypothesis based on the data presented: "Access control measures, including MFA, are used to manage access to open data platforms in the Republic of Kosovo." The proportion of access control measures used shows that institutions have employed a variety of policies and technologies to secure access to these sites. Multi-factor authentication is a cybersecurity strategy that helps protect data and is widely utilized by numerous institutions. This validation of MFA use on open data platforms for access control verifies our theory.

Hypothesis 4: Open data platforms in the Republic of Kosovo are regularly accessed by the public and stakeholders for a variety of use cases.

In the Republic of Kosovo, users of open data platforms utilize them for a variety of purposes. For example, 27.2% of respondents said they used the platforms for application development, while 25.9% said they used them for professional consultation. This usage distribution demonstrates a strong interest in leveraging open data platforms for a variety of applications (see Table 4).

Table 4. Public access to Kosovo data

What are the Main Use Cases for this Platform?		Responses		Percent of Cases
		N	Percent	
H4[a]	Answering questions	13	16.0%	21.7%
	Professional advice	21	25.9%	35.0%
	Application development	22	27.2%	36.7%
	Information Research	19	23.5%	31.7%
	Fast customer service.	6	7.4%	10.0%
Total		81	100.0%	135.0%

Note: [a]Dichotomy group tabulated at value 1.

The findings support our hypothesis that open data platforms in the Republic of Kosovo are regularly accessed by the general public and stakeholders for a variety of use cases. The high proportion of platform utilization for application development and professional consultation indicates that these platforms are in great demand and are actively used by consumers. This implies that these platforms should be used regularly for a variety of purposes, including creating applications and retrieving information.

Hypothesis 5: Data quality control measures are implemented on open data platforms in the Republic of Kosovo.

Based on the findings of the table above, it is clear that careful precautions are taken to ensure data quality in open data platforms on the Republic of Kosovo. For example, 66.7% of respondents say data security is an essential factor, and 60.0% say performance monitoring is an important tool to ensure quality. In addition to security and performance monitoring, data is crucial for ethics and transparency, as 8.3% of respondents consider user guideline distribution as another important factor. This component assists users in interpreting and using data appropriately and ethically. Overall, these findings reflect the commitment of the institutions in the Republic of Kosovo to ensuring the quality and integrity of open data. They confirm our hypothesis that data quality control measures, along with security measures, are implemented on open data platforms in the Republic of Kosovo (see Table 5).

Table 5. Kosovo data quality controls

How is the Accuracy and Reliability of the Data Offered on the Platform Ensured?				
		Responses		Percent of Cases
		N	Percent	
H2.1[a]	Performance monitoring	36	26.9%	60.0%
	Error correction	23	17.2%	38.3%
	Data security	40	29.9%	66.7%
	Ethics and transparency	5	3.7%	8.3%
	User guidance and instructions.	30	22.4%	50.0%
Total		134	100.0%	223.3%

Note: [a]Dichotomy group tabulated at value 1.

The results of this analysis confirm our hypothesis that data quality control measures are implemented on open data platforms in the Republic of Kosovo. The high percentage of responses related to data security and performance monitoring indicates that these quality measures are present and carefully applied on open data platforms in the Republic of Kosovo. This is an important intervention to ensure that the presented data is accurate and reliable for users.

Hypothesis 6: Public institutions in the Republic of Kosovo collect and utilize feedback from users to improve open data platforms.

Based on the findings, the majority of users of open data platforms in the Republic of Kosovo have captured the interest of institutions through their comments and evaluations. This is evident because 56.7% of respondents indicated that they regularly engage with institutions through comments and ratings. Indeed, regular user participation is evident, with 23.3% of users reporting that they contribute comments and reviews to open data platforms on a daily or frequent basis (see Table 6).

Table 6. Kosovo institutions improve data platforms

Do you Gather Comments and Feedback from Users of the Open Data Platform?	N	%
Very rarely	7	11.7
Rarely	19	31.7
Average	16	26.7
Often	14	23.3
Always	4	6.7

This supports our premise that governmental organizations in the Republic of Kosovo receive user feedback and ratings to enhance open data platforms. This approach is critical for ensuring that platforms provide what consumers want and need, thereby enhancing usability and data quality.

Hypothesis 7: Collaborations exist to enhance open data platforms in the Republic of Kosovo.

According to the findings, collaborations on open data platforms in the Republic of Kosovo focus on several critical factors, including strategic alliances, developer space, usage monitoring and analysis, and continuous feedback and improvements. Strategic alliances have a significant impact on platform efficiency as they bring in new resources, knowledge, and increased consumption. The developer environment fosters creativity and the development of third-party apps, while the utilization of monitoring and analysis allows institutions to assess effectiveness and implement enhancements. Continuous feedback and changes demonstrate institutions' commitment to meeting user expectations, enhancing security, and safeguarding privacy. Simultaneously, capacity expansion enhances platform management capabilities and resources (see Table 7).

Table 7. Kosovo collaborates for data enhancement

How are these Collaborations Managed, and How do they Impact the Efficiency of the Platform?				
		Responses		Percent of Cases
		N	Percent	
H7[a]	Strategic partnerships	14	18.7%	31.1%
	Space for developers	11	14.7%	24.4%
	Community building	5	6.7%	11.1%
	Monitoring and usage analysis	13	17.3%	28.9%
	Feedback and continuous improvements	9	12.0%	20.0%
	Development of advanced learning models	9	12.0%	20.0%
	Security and privacy	5	6.7%	11.1%
	Capacity building.	9	12.0%	20.0%
Total		75	100.0%	166.7%

Note: [a]Dichotomy group tabulated at value 1.

These findings support our premise that cooperation to enhance open data platforms exists in the Republic of Kosovo. The content and actions of partnerships and development areas demonstrate that institutions are making significant efforts to improve the efficiency and utility of their open data platforms. This is a critical factor in enhancing services and usability for the general public and entrepreneurs, leading to increased usage and a positive impact on society and decision-making.

Hypothesis 8: Public institutions in the Republic of Kosovo have methods to measure the impact and effectiveness of open data initiatives and can provide examples of their benefits.

The findings indicate that public organizations in the Republic of Kosovo use a variety of methodologies to analyze the effectiveness and impact of their open data initiatives. A significant number of them monitor and evaluate platform usage, and many set specific goals and objectives. User input and assessments are utilized to make improvements. In general, employing these strategies is a crucial step in managing and enhancing open data programs (see Table 8).

Table 8. Kosovo evaluates open data impact

How are the Impact and Effectiveness of Open Data Initiatives Evaluated?				
		Responses		Percent of Cases
		N	Percent	
8	Setting goals and objectives	12	20.0%	20.0%
	Monitoring and assessing usage	22	36.7%	36.7%
	Gathering feedback and user assessments	13	21.7%	21.7%
	Analyzing success cases	1	1.7%	1.7%
	Reviewing and improving the initiative.	12	20.0%	20.0%
Total		60	100.0%	100.0%

Note: [a]Dichotomy group tabulated at value 1.

These findings support our hypothesis that public organizations in the Republic of Kosovo have procedures for evaluating the impact and success of their open data efforts. Monitoring and evaluating usage have been successfully employed to examine how these platforms are used and their impact on decision-making and society. User input and evaluation are also important tools for improving and adapting open data platforms in the Republic of Kosovo. These activities reflect institutions' dedication to improving the effectiveness and assessment of their open data programs.

Hypothesis 9: Privacy measures are in place to safeguard individuals' data on open data platforms in the Republic of Kosovo.

The findings demonstrate that public organizations in the Republic of Kosovo handle personally identifiable information (PII) on open data platforms responsibly. The organization with the highest number of replies demonstrates efficient data identification and categorization, as well as a strong commitment to data security. They also invest in staff training to ensure that personal information is handled with care and protection. Furthermore, some companies use security breach prevention methods to maintain data integrity. These institutions' commitment indicates their responsible approach toward individual privacy and data security on open data platforms in the Republic of Kosovo (see Table 9).

Table 9. Kosovo ensures open data privacy

How is Personally Identifiable Information (PII) Handled, and What is the Institution's Role in this Process?				
		Responses		Percent of Cases
		N	Percent	
H9[a]	Identification and classification of data	39	33.3%	72.2%
	Data security	30	25.6%	55.6%
	Auditing and monitoring	9	7.7%	16.7%
	Personnel training	24	20.5%	44.4%
	Protection against security breaches	15	12.8%	27.8%
Total		117	100.0%	216.7%

Note: [a]Dichotomy group tabulated at value 1.

These findings support our hypothesis that privacy safeguards are implemented to protect individuals' data on open data platforms in the Republic of Kosovo. Institutions are involved in identifying and categorizing personal data, and they are committed to maintaining the security and integrity of this data. Staff training and security standards reflect efforts to improve the handling of personally identifiable information on these sites.

Hypothesis 10: Data ownership is clearly defined in the data management policies for open data platforms in the Republic of Kosovo.

According to the findings, the majority of the data posted on the Republic of Kosovo's open data platform is held by government entities or government agencies. This demonstrates the importance of government organizations in delivering data to users. However, it is vital to note that a certain amount of data is held by individuals or application developers, showcasing an open and diverse contributor base to these platforms. Simultaneously, the majority of replies suggest a distinct absence of a definition of data ownership in institutional data management rules (see Table 10).

Table 10. Kosovo defines open data ownership

Who Owns the Data Placed on the Open Data Platform?				
		Responses		Percent of Cases
		N	Percent	
H10[a]	Government organization or government institution	43	68.3%	81.1%
	Open community or the public	6	9.5%	11.3%
	Academic or scientific institutions	4	6.3%	7.5%
	Individuals or application developers	9	14.3%	17.0%
	Is data ownership clearly defined in the data management policy of the institution?	1	1.6%	1.9%
Total		63	100.0%	118.9%

Note: [a]Dichotomy group tabulated at value 1.

These findings support our hypothesis that data ownership is inadequately specified in institutions' data management policies on open data platforms in the Republic of Kosovo. Even though government entities predominantly share data, the lack of clarity in data ownership policies indicates the necessity for change and a more comprehensive explanation of the norms and responsibilities associated with data ownership and usage on these platforms.

Hypothesis 11: Open data platforms in the Republic of Kosovo cover a wide range of public service areas with significant data volumes.

The results show that the open data platform in the Republic of Kosovo is data-rich, with a high number of responses indicating that it contains a vast amount of data. It's also worth noting that the majority of responses suggest a large number of data sets. This fact demonstrates that the Republic of Kosovo's open data platform is filled with a diverse set of data covering a wide range of public service topics (see Table 11).

Table 11. Kosovo drivers, voluminous open data

How Extensive is the Open Data Platform in Terms of Data Quantity and the Number of Data Sets?				
		Responses		Percent of Cases
		N	Percent	
H11[a]	Platform with a large quantity of data	37	58.7%	61.7%
	Platform with limited data quantity	21	33.3%	35.0%
	Platform with a large number of data sets	2	3.2%	3.3%
	Platform with distributed and open data	3	4.8%	5.0%
Total		63	100.0%	105.0%

Note: [a]Dichotomy group tabulated at value 1.

These findings support our hypothesis that the open data platform of the Republic of Kosovo covers a wide range of public service domains with a substantial amount of data. This is critical for increasing the openness and accessibility of these platforms, which serve as a rich source of information for the general public and enterprises.

Hypothesis 12: Public institutions in the Republic of Kosovo face challenges in maintaining secure and effective open data platforms and have recognized opportunities for enhancement.

The findings reveal that institutions in the Republic of Kosovo face several significant obstacles in maintaining a secure and successful open data platform. A significant number of responses indicate that the main challenges they encounter are privacy and data security. This demonstrates that data security and protecting individuals' privacy are critical objectives for organizations when dealing with open data. Furthermore, coordination and partnership issues are acknowledged as crucial interventions, emphasizing the importance of effective collaboration and coordination among governmental agencies and organizations. In addition to resources and financing, which are important variables in sustaining open data platforms, user education and awareness have been cited as challenges (see Table 12).

Table 12. Kosovo addresses open data challenges

What are the Main Challenges your Institution Faces in Maintaining a Secure and Efficient Open Data Platform in the Republic of Kosovo?		Responses		Percent of Cases
		N	Percent	
H12[a]	Privacy protection	25	20.2%	42.4%
	Data security	10	8.1%	16.9%
	Coordination and partnerships	19	15.3%	32.2%
	User education and awareness	30	24.2%	50.8%
	Resources and funding	40	32.3%	67.8%
Total		124	100.0%	210.2%

Note: [a]Dichotomy group tabulated at value 1.

In these circumstances, the findings of this study support the notion that institutions in the Republic of Kosovo face a variety of challenges in maintaining open data platforms, as well as opportunities for growth. This covers issues related to security and privacy, coordination and collaboration, user awareness, and the necessity for increased resources and financing. By addressing these obstacles and capitalizing on opportunities for development, institutions in the Republic of Kosovo can enhance the effectiveness and security of their open data platforms.

5 DISCUSSIONS

Transparency, innovation, and improved public engagement is all advantages of open data platforms. However, issues such as data privacy, data quality, and data security must be addressed. Best practices include robust security measures, access limits, and user authentication, as demonstrated by systems such as data.gov.au in Australia and Data.gov in the United States, which emphasize constant monitoring. Open data in the commercial sector facilitates market analysis and product development, highlighting the need for cybersecurity solutions that prioritize threat detection and prevention. Collaboration and data sharing on open data platforms help exchange knowledge and foster innovation. Privacy issues, as exemplified by New York City's difficulties, underscore the need for a balance between the advantages of open data and individual privacy, supported by the General Data Protection Regulation (GDPR). Businesses encounter challenges such as data quality and security, highlighting the significance of ethical data practices. To counteract growing threats, cybersecurity is critical. Strong recommendations include implementing rigorous access restrictions, encryption, and continual monitoring. Data anonymization protects privacy, which is critical for complying with regulations and implementing effective security measures. Proposals emphasize the importance of data quality, cooperation, and ethical concerns. They stress the significance of ethical frameworks, user-centered design, and continuous monitoring in responsible data management. Public entities in the Republic of Kosovo invest in cybersecurity measures, encryption, and access requirements, emphasizing the significance of constant monitoring for successful cybersecurity systems.

6 CONCLUSIONS

The need for cybersecurity in open data platforms is crucial for preserving data integrity and user confidence. While these platforms provide openness, innovation, and public involvement, they also pose data privacy and security issues. Comprehensive solutions, such as access limits, encryption, and continual monitoring, are required to protect open data. Government programs spur innovation, but there are issues with data quality and sustainability. Emerging technologies such as artificial intelligence (AI) and blockchain are shaping open data ecosystems, highlighting the ongoing need to address privacy and ethical issues. Organizations must prioritize security in the face of emerging cyber threats by implementing access limits, encryption, and constant monitoring. Data anonymization and stringent privacy safeguards are crucial for protecting sensitive information. To develop confidence and enhance utility, data quality, especially in the public sector, requires investments in management and quality control. Standardized data formats and efficient data management enable seamless integration for the benefit of society. Continuous investments and creative financial strategies are required to ensure long-term access to critical data. For the appropriate use of open data, ethical issues related to fairness and transparency are crucial. Individual control over privacy settings is prioritized to enhance user-centricity, foster trust, and informed decision-making. Maintaining trust, data integrity, and flexibility requires regular privacy evaluations and ethical enforcement. Public institutions in the Republic of Kosovo address cybersecurity and data quality issues by implementing solutions such as data identification, encryption, and access control. Partnerships on open data platforms have a significant impact on Kosovo. However, more clarity on data ownership and improvements in personal data security are required.

7 RECOMMENDATIONS

Cybersecurity in open data is a potent tool for fostering transparency, innovation, and informed decision-making. As these platforms evolve, addressing multifaceted challenges and ethical considerations regarding data privacy, security, and data accuracy becomes imperative. The following concise recommendations emphasize the pivotal role of robust cybersecurity, data privacy, data accuracy, and collaborative engagement among stakeholders. These structured guidelines are intended to assist governments, organizations, and individuals in effectively navigating the intricate landscape of open data:

1. Strengthen cybersecurity measures
2. Promote data privacy
3. Enhance data quality
4. Facilitate collaboration
5. Protect open data platforms
6. Maintain a balanced approach
7. Ethical considerations and ethical frameworks
8. User-centered design
9. Effective data management
10. Education and awareness
11. Continuous monitoring and auditing

The Republic of Kosovo has made significant progress in developing and improving open data platforms. Although there is potential for improvement in various areas, such as encryption, awareness, and staff training, collaborative management is one aspect in which cloud facilities can better and more effectively utilize of these open information resources.

Recommendations derived from the hypotheses:

- The Republic of Kosovo's public institutions should continue to enhance their cybersecurity policies and ensure that they are regularly updated to address emerging threats.
- To enhance cybersecurity, institutions should implement awareness practices among their personnel and share expertise to mitigate the risk of cybersecurity breaches.
- Data quality measures, such as performance monitoring and data security, should be enhanced and advanced to ensure excellent data quality for open data. Institutions should continue to collect user input and evaluate open data platforms to identify potential areas for improvement.
- Fostering cooperation and strengthening collaborations will enhance the efficiency and value of open data platforms.
- Institutions should continue to encourage users to provide comments and assessments, establish effective communication with users, and assess feedback to pinpoint areas requiring further enhancement to strengthen open data platforms in the Republic of Kosovo.
- Effective monitoring and assessment should be implemented. Institutions should continue to apply these methods to enhance open data platforms and showcase their value to the general public and entrepreneurs.

8 REFERENCES

[1] B. Hyseni and L. A. Bexheti, "The impact of open data standardization on the successful management of e-government," in *12th Mediterranean Conference on Embedded Computing (MECO)*, 2023. https://doi.org/10.1109/MECO58584.2023.10154925

[2] A. Zwitter, "Big data ethics," *Big Data & Society*, vol. 1, p. 2053951714559253, 2014. https://doi.org/10.1177/2053951714559253

[3] A. Zuiderwijk, M. Janssen, S. Choenni, R. Meijer, and R. S. Alibaks, "Socio-technical impediments of open data," *Electronic Journal of e-Government*, vol. 10, pp. 156–172, 2012.

[4] S. Verhulst and A. Young, "Open data impact when demand and supply meet key findings of the open data impact case studies," *SSRN*, p. 3141474, 2016.

[5] G. Vancauwenberghe and J. Crompvoets, "Governance of open data initiatives," in *Open Data Exposed,* The Hague: T.M.C. Asser Press, 2018, pp. 79–100. https://doi.org/10.1007/978-94-6265-261-3_5

[6] J. Van Dijck and T. Poell, "Understanding social media logic," *Media and Communication*, vol. 1, pp. 2–14, 2013. https://doi.org/10.17645/mac.v1i1.70

[7] B. Ubaldi, "Open government data: Towards an empirical analysis of open government data initiatives," OECD Working Papers on Public Governance No. 22, 2013.

[8] S. M. T. Toapanta, J. M. E. Jaramillo, and L. E. M. Gallegos, "Cybersecurity analysis to determine the impact on the social area in Latin America and the Caribbean," in *Proceedings of the 2019 2nd International Conference on Education Technology Management*, 2019. https://doi.org/10.1145/3375900.3375911

[9] L. Taylor and D. Broeders, "In the name of development: Power, profit and the ratification of the global south," *Geoforum*, vol. 64, pp. 229–237, 2015. https://doi.org/10.1016/j.geoforum.2015.07.002

[10] J. Tauberer, E. Mill, J. Gray, P. Higgins, M. Weinberg, and T. Vollmer, "Open government data: Best-practices language for making data 'license-free'," *Open Government Data*, vol. 13, 2013.

[11] N. Tariq, M. Asim, F. Al-Obeidat, M. Zubair Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors*, vol. 19, p. 1788, 2019. https://doi.org/10.3390/s19081788

[12] D. J. Solove, "Understanding privacy," 2008. https://ssrn.com/abstract=1127888

[13] P. Regulation, "General data protection regulation," *Intouch*, vol. 25, pp. 1–5, 2018.

[14] R. Raimundo and A. Rosário, "The impact of artificial intelligence on data system security: A literature review," *Sensors*, vol. 21, p. 7029, 2021. https://doi.org/10.3390/s21217029

[15] N. A. Osman, S. A. Mohd Noah, M. Darwich, and M. Mohd, "Integrating contextual sentiment analysis in collaborative recommender systems," *Plos One*, vol. 16, p. e0248695, 2021. https://doi.org/10.1371/journal.pone.0248695

[16] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA Law Review*, vol. 57, pp. 1701–1777, 2009.

[17] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *IEEE Symposium on Security and Privacy*, 2008. https://doi.org/10.1109/SP.2008.33

[18] T. Nam and T. A. Pardo, "Conceptualizing smart city with dimensions of technology, people, and institutions," in *Proceedings of the 12th annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*, 2011. https://doi.org/10.1145/2037556.2037602

[19] K. Mossberger, C. J. Tolbert, and R. S. McNeal, *Digital Citizenship, The Internet, Society, and Participation*. Cambridge, MA: MIT Press, 2007. https://doi.org/10.7551/mitpress/7428.001.0001

[20] M. Mayernik, "Open data: Accountability and transparency," *Big Data & Society*, vol. 4, p. 205395171771885, 2017. https://doi.org/10.1177/2053951717718853

[21] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. Hung Byers, "Big data: The next frontier for innovation, competition, and productivity," McKinsey Global Institute, Seattle, 2011.

[22] K. Lee, "Workplace Gender Equality Agency—Progress Report 2019–20," Commonwealth of Australia, 2021.

[23] D. Lee, "Public data analysis and utilization," *International Research Journal of Engineering and Technology (IRJET)*, vol. 9, no. 2, pp. 893–898, 2022.

[24] D. Lathrop and L. Ruma, *Open Government: Collaboration, Transparency, and Participation in Practice*. Sebastopol, CA: O'Reilly Media, 2010.

[25] K. Lanson, *The Routledge Companion to Mobile Media Art*. Routledge, 2020. https://doi.org/10.4324/9780429242816-1

[26] J. A. Kroll, "Accountable algorithms," Doctoral Dissertation, Princeton University, 2015. http://arks.princeton.edu/ark:/88435/dsp014b29b837r

[27] R. Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. Thousand Oaks, California: Sage Publications, 2014, pp. 1–240. https://doi.org/10.4135/9781473909472

[28] M. P. Kato, H. Ohshima, Y.-H. Liu, and H.-L. Chen, "A test collection for ad-hoc dataset retrieval," in *Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval*, 2021, pp. 2450–2456. https://doi.org/10.1145/3404835.3463261

[29] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet of Things Journal*, vol. 7, pp. 10250–10276, 2020. https://doi.org/10.1109/JIOT.2020.2997651

[30] J. Gurin, *Open Data Now: The Secret to Hot Startups, Smart Investing, Savvy Marketing, and Fast Innovation*. New York, NY: Mc Graw Hill, 2014.

[31] M. F. Goodchild, "Citizens as sensors: The world of volunteered geography," *GeoJournal*, vol. 69, pp. 211–221, 2007. https://doi.org/10.1007/s10708-007-9111-y

[32] A. Fung, M. Graham, and D. Weil, *Full Disclosure: The Perils and Promise of Transparency*. Cambridge: Cambridge University Press, 2007. https://doi.org/10.1017/CBO9780511510533

[33] L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. New York, NY: OUP Oxford, 2014.

[34] S. Feuerriegel, M. Dolata, and G. Schwabe, "Fair AI: Challenges and opportunities," *Business & Information Systems Engineering*, vol. 62, pp. 379–384, 2020. https://doi.org/10.1007/s12599-020-00650-3

[35] F. Ferri, "The dark side (s) of the EU Directive on copyright and related rights in the digital single market," *China-EU Law Journal*, vol. 7, pp. 21–38, 2021. https://doi.org/10.1007/s12689-020-00089-5

[36] K. El Emam and L. Arbuckle, *Anonymizing Health Data: Case Studies and Methods to Get You Started*. Sebastopol, CA: O'Reilly Media, Inc., 2013.

[37] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of Models of Computation*, 2008.

[38] N. Diakopoulos, "Algorithmic accountability: A primer," Data Society Research Institute, 2016.

[39] M. Chui, J. Manyika, and M. Miremadi, "Where machines could replace humans where they can't (yet)," *McKinsey Quarterly*, 2016.

[40] X. Chen, L. Zhang, Y. Zhang, J. Du, X. Jia, and X. Yang, "A fundamental analysis of standardization for blockchain and distributed ledger technologies in ISO," in *9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2022. https://doi.org/10.1109/CSCloud-EdgeCom54986.2022.00016

[41] H.-C. Chen, A. M. Widodo, A. Wisnujati, M. Rahaman, J. C.-W. Lin, L. Chen, and C.-E. Weng, "AlexNet convolutional neural network for disease detection and classification of tomato leaf," *Electronics*, vol. 11, p. 951, 2022. https://doi.org/10.3390/electronics11060951

[42] J. Carlo Bertot, P. T. Jaeger, and J. M. Grimes, "Promoting transparency and accountability through ICTs, social media, and collaborative e-government," *Transforming Government: People, Process and Policy*, vol. 6, pp. 78–91, 2012. https://doi.org/10.1108/17506161211214831

[43] M. Cao, R. Chychyla, and T. Stewart, "Big data analytics in financial statement audits," *Accounting Horizons*, vol. 29, pp. 423–429, 2015. https://doi.org/10.2308/acch-51068

[44] J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms," *Big Data & Society*, vol. 3, p. 2053951715622512, 2016. https://doi.org/10.1177/2053951715622512

[45] R. Brym, M. Godbout, A. Hoffbauer, G. Menard, and T. H. Zhang, "Social media in the 2011 Egyptian uprising," *The British Journal of Sociology*, vol. 65, pp. 266–292, 2014. https://doi.org/10.1111/1468-4446.12080

[46] B. Brown, J. Bughin, A. H. Byers, M. Chui, R. Dobbs, J. Manyika, and C. Roxburgh, "Big data: The next frontier for innovation, competition, and productivity," McKinsey Global Institute, Seattle, pp. 1–156, 2011.

[47] B. Ansari, M. Barati, and E. G. Martin, "Enhancing the usability and usefulness of open government data: A comprehensive review of the state of open government data visualization research," *Government Information Quarterly*, vol. 39, p. 101657, 2022. https://doi.org/10.1016/j.giq.2021.101657

[48] B. Hyseni and L. A. Bexheti, "Perspective of open data application in Republic of Kosovo, challenges, and advantages," in *11th Mediterranean Conference on Embedded Computing (MECO)*, 2022. https://doi.org/10.1109/MECO55406.2022.9797194

9 AUTHORS

Besart Hyseni, Ph.D. Candidate, Faculty of Contemporary Sciences and Technologies, South East European University, Tetovo, North Macedonia (E-mail: bh29738@seeu.edu.mk).

Prof. Dr. Ing. Lejla Abazi Bexheti, Faculty of Contemporary Sciences and Technologies, South East European University, Tetovo, North Macedonia (E-mail: l.abazi@seeu.eduk.mk).