Real-Time Data Governance and Compliance in Cloud-Native Robotics Systems

UNDER PEER REVIEW

Abstract

This study investigates the frameworks and challenges of real-time data governance and compliance in cloud-native robotics systems, focusing on data integrity, cloud security, regulatory adherence, and cybersecurity risks. Using extensive datasets from the Amazon AWS Open Data Registry, the EU GDPR Enforcement Tracker, and Kaggle's IoT dataset, the analysis explores cloud-native systems' data accuracy, security, and governance. Data were extracted through a standardized process: performance metrics, including latency and error rates, were gathered from Amazon AWS to assess system efficiency, GDPR violation records were analyzed from the EU Enforcement Tracker to understand compliance trends, and data volume and governance metrics from Kaggle's IoT dataset were correlated to identify governance challenges. Together, these data sources provide comprehensive insights into how cloud-native systems can be optimized for real-time operations. The study highlights the cloud security benefits and governance advantages inherent to cloud-native frameworks, such as real-time monitoring, automated threat detection, and data encryption, which collectively reduce unauthorized access risks while supporting operational efficiency. Findings indicate high data accuracy (0.51% error rate) and low latency (mean of 48.96 ms) across systems; however, processing time variability (standard deviation of 28.61 ms) signals a need for further optimization in time-sensitive environments. The regression analysis of GDPR violations reveals a substantial penalty increase of €53,789.41 per violation, emphasizing the financial risks of non-compliance. Correlation analysis (r = 0.083 for data volume and governance failures) suggests that external cybersecurity threats have a greater impact on governance than internal metrics, underscoring the importance of adaptive governance frameworks that support both data integrity and regulatory compliance in cloud-native robotics systems.

Keywords: Real-Time Data Governance, Cloud-Native Robotics, GDPR Compliance, Cybersecurity, Data Integrity.

1.Introduction

The rapid advancement of robotics and autonomous systems has significantly transformed industries such as manufacturing, healthcare, and transportation, and central to this transformation is the integration of cloud-native technologies, which enable robotic systems to utilize cloud-based infrastructure for processing, decision-making, and data storage. Cloud infrastructure offers scalability, flexibility, and real-time data management capabilities, essential for robots operating in dynamic environments. However, these advancements also bring significant challenges in terms of data governance and regulatory compliance, particularly concerning data integrity, security, and privacy. According to Polamarasetti [1], as cloud-native robotics systems grow in complexity, ensuring robust data governance frameworks becomes increasingly critical.

Data governance in cloud-native robotics systems involves managing large volumes of diverse data, including sensor inputs, operational metrics, and user interactions. The sheer volume and velocity of this data pose challenges in maintaining its quality, accuracy, and integrity. Anumbe et al. [2] posit that these factors are crucial to ensuring that robotic systems make optimal real-time decisions. For example, Amazon Robotics relies on AWS to manage its robot fleets in fulfillment centers, where vast amounts of data are processed to streamline operations, and any issue with data accuracy or latency can have significant operational and decision-making consequences, as noted by Keung et al. [3].

As robotics systems increasingly adopt cloud-native architectures, concerns over data security and privacy become more pronounced. The distributed nature of cloud environments requires constant data exchange between robots and cloud servers, which exposes information to risks such as breaches, unauthorized access, and cyberattacks. Muhammad et al. [4] reference the 2021 Tesla Model S hack as a case demonstrating the vulnerability of autonomous vehicles to cyber threats. Similarly, in 2022, data breaches at robotics companies in healthcare and manufacturing exposed sensitive data [5]. These incidents showcase the need for strict security measures to protect real-time data in cloud-native robotics systems, as noted by Hossain et al. [6].

In cloud-native robotics, robust governance frameworks serve as essential safeguards, ensuring data security, risk management, and operational stability [6][7]. These frameworks not only uphold regulatory compliance but also bolster data integrity by implementing controls on data access, encryption, and lifecycle management. The application of cloud governance standards supports organizations in reducing vulnerabilities while enabling efficient, secure data flows in real time [7][8].

Bakare et al. [7] also highlight the additional challenge of compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). These regulations impose strict standards on the handling of sensitive data, often collected by autonomous

UNDER PEER REVIEW

systems. For example, Tesla faced legal scrutiny in 2023 for collecting customer data, including dashcam footage, without proper consent. This illustrated the risks of non-compliance, and Radanliev [8] states that adherence to these regulations is essential to maintain legal compliance and public trust in cloud-native robotics.

Scalability represents another key factor in the effective governance of cloud-native robotics systems. These systems are designed to handle fluctuating data volumes and operational workloads, allowing them to adapt to changing demands. Bathla et al. [9] argue that Waymo's self-driving vehicles, which generate substantial amounts of data processed in the cloud, exemplify the need for scalability. However, the growing volume of data presents governance challenges. As data volumes expand, organizations must ensure that their capacity to manage and secure data grows accordingly. De Filipii et al. [10] contend that failing to address these governance issues could compromise system reliability and security.

Real-time data processing further complicates data governance in cloud-native robotics. These systems must process and act on data instantaneously, often in unpredictable environments, creating tension between the need for fast decision-making and the requirement for rigorous data oversight. Theodorakopoulos et al. [11] suggest that this challenge is particularly relevant in systems like Amazon Robotics, which rely on real-time data to optimize operations. Without strong governance, data inaccuracies or delays could lead to operational inefficiencies and safety risks. Thus, according to Radanliev [8], robust governance practices are essential for maintaining both accuracy and efficiency in real-time environments.

Technologies such as artificial intelligence (AI), machine learning (ML), and edge computing are introducing new complexities to data governance. Though these technologies enhance the capabilities of robotics systems, they also present additional risks related to data accuracy and security. Dwivedi et al. [12] posit that the rapid pace of technological advancement necessitates ongoing updates to governance frameworks to address these challenges. Without continuous reassessment, governance frameworks may become outdated, leaving systems vulnerable to emerging risks.

Data integration and interoperability also pose significant challenges in cloud-native robotics, as these systems rely on diverse data sources, including cloud infrastructures and on-device sensors, which must work together seamlessly to support decision-making. However, ensuring the quality, consistency, and accuracy of this data is challenging due to potential issues such as sensor noise, network latency, and data anomalies. Radanliev [8] argues that developing robust governance frameworks to manage the integration of diverse data streams is critical for maintaining data accuracy and consistency.

UNDER PEER REVIEW

Addressing these challenges requires a multifaceted approach that combines technological solutions, organizational policies, and regulatory compliance. Radanliev [8] asserts that organizations must implement best practices in data governance, such as real-time monitoring, encryption, and automated data validation, to ensure the secure and efficient operation of cloud-native robotics systems. As these systems become increasingly integrated into various industries, Kaplan [82] asserts that the development of advanced governance frameworks will be essential for mitigating risks and maintaining system reliability.

The rapid adoption of cloud-native robotics systems introduces complex challenges for data governance frameworks, particularly in the face of escalating cybersecurity threats. As these systems handle vast, real-time data transfers between cloud and edge devices, they become highly susceptible to unauthorized access and data breaches, which can lead to significant governance failures. Addressing these vulnerabilities requires a rethinking of current governance practices to prioritize both data security and compliance, ensuring operational integrity in cloud-native robotics environments. Therefore, this study aims to explore and evaluate the frameworks, challenges, and best practices for implementing real-time data governance and compliance in cloud-native robotics systems; the study achieves the following objectives:

1. Examines the key principles of real-time data governance in cloud-native robotics systems.
2. Analyses the regulatory frameworks and compliance standards that impact cloud-native robotics systems.
3. Identify and assess the challenges associated with integrating real-time data governance practices in cloud-native robotic operations and propose potential solutions to address these challenges.
4. Develops a framework of best practices for implementing effective data governance and ensuring compliance in real-time cloud-native robotics systems.

2. Literature Review

Real-time data governance is essential for the efficient functioning of cloud-native robotics systems, ensuring the accuracy, security, and reliability of the data driving these technologies. In this context, data governance refers to a framework of policies, processes, and standards that manage data availability, usability, integrity, and security. Das and Mukherjee [13] argue that given the dynamic nature of cloud-native robotics, where real-time decision-making is critical, maintaining data integrity and security is paramount because errors in data can result in flawed decisions, leading to operational inefficiencies and safety risks. Thus, real-time data governance plays a crucial role in mitigating such risks.

UNDER PEER REVIEW

The core principles of real-time data governance include ensuring data quality, integrity, accuracy, and security, and according to Theodorakopoulos et al. [11], these factors guarantee that robotic systems can depend on consistent and uncorrupted data to function optimally. Konstas et al. [14] posit that any deviation in data quality or accuracy may lead to faulty decision-making, thereby negatively impacting operations. Integrity, on the other hand, ensures that data remains consistent and untampered throughout its lifecycle. At the same time, security safeguards it against unauthorized access, especially in the face of increasing cyber threats targeting cloud-based systems [15][16].]

A notable example of the importance of real-time data governance can be observed in Amazon Robotics, which utilizes cloud-native infrastructure to manage its robotic fleet in fulfillment centers. Sheu and Choi [17] aver that these robots rely heavily on real-time data streams for tasks such as inventory management and order fulfilment, and data errors, such as incorrect inventory counts or sensor anomalies, could disrupt operations, which emphasizes the need for robust data governance [18][19]. Aldoseri et al. [20] note that Amazon employs data quality checks, anomaly detection algorithms, and real-time validation techniques to mitigate these risks and maintain operational efficiency.

The integration of emerging technologies such as artificial intelligence (AI), machine learning (ML), and edge computing has further enhanced the complexity of data governance frameworks [21][22]. Although AI and ML can automate data quality checks and optimize decision-making processes, they also introduce new challenges, particularly when it comes to ensuring that these models function correctly [20][23][24]. Seng et al. [25] contend that the effectiveness of these models depends on high-quality, accurate data. Moreover, edge computing, which processes data closer to its source to reduce latency, enhances real-time responsiveness but adds complexity to governance frameworks by increasing the number of data collection points, making secure oversight more challenging [26][27].

Cloud governance frameworks, including policies on data access, classification, and encryption, play an integral role in managing risks within robotics systems. Such policies provide standards that support data integrity, enhance transparency, and mitigate unauthorized access risks in cloud-native infrastructures [26][28]. By setting these rules, organizations can better align their operations with compliance requirements, as well as secure data in distributed cloud and edge environments where data transfers are rapid and frequent. As cloud-native robotics systems develop, the frameworks governing their data must evolve accordingly [28][29]. The vast volume and rapid generation of real-time data by robotic systems intensify the challenges of maintaining consistent quality and security. Artificial intelligence (AI), machine learning (ML), and edge computingare offering opportunities to automate and improve governance processes, but they also require careful management to address

UNDER PEER REVIEW

the complexities they introduce. Johnson et al. [30] argue that the scalability of governance frameworks is essential, as they must not only meet current demands but also accommodate the increasing complexity of real-time data environments, and this ensures that robotic systems continue to function efficiently and securely amid advancing technological developments [31][32].

Cybersecurity in Cloud-Native Robotics Systems

Cybersecurity is a critical concern for cloud-native robotics systems due to their increasing exposure to threats ranging from data tampering to unauthorized control of operations. These systems, with their interconnected structure and real-time data transmission, face heightened vulnerability to cyberattacks, as cited by [33][34][35]. Tuyishime et al. [36] argue that cloud-native systems' continuous data exchange between robots and cloud servers expands the potential attack surface, thereby increasing the risks of data breaches, unauthorized access, and operational failures. While this persistent flow of data is essential for real-time decision-making, it also presents significant security challenges [37][38].

The distributed nature of cloud-native systems further worsens their susceptibility to cyberattacks. Attackers can alter or intercept data before it reaches its intended destination, a scenario that can severely disrupt real-time applications [39][40]. According to Shahid et al. [41], delays or inaccuracies in data transmission caused by such attacks can compromise decision-making processes, particularly in sensitive settings like healthcare, where a compromised robot transmitting patient data could lead to incorrect diagnoses or treatments. Therefore, Saurabh et al. [42] contend that robust cybersecurity frameworks incorporating real-time monitoring and advanced intrusion detection systems (IDS) are essential to mitigate these risks. Encryption is another key component, ensuring data integrity and confidentiality by making it more difficult for attackers to manipulate or intercept sensitive information [43][44].

The integration of artificial intelligence (AI) and machine learning into cybersecurity frameworks has marked a significant advancement in securing cloud-native robotics systems. AI-driven security systems, as Goswami [45] avers, can analyze large volumes of real-time data and detect anomalies more efficiently than traditional methods. These systems learn from previous attack patterns, enabling them to anticipate future threats and provide proactive defense mechanisms [46][47]; machine learning models, as they continuously adapt to new attack strategies, offer a critical advantage in unpredictable environments, such as autonomous vehicles [9][48]. Joao et al. [49] posit that AI-based security frameworks offer a faster and more adaptive defense against evolving cyber threats, which improves the protection of critical robotics operations.

UNDER PEER REVIEW

However, despite these advancements in security technologies, Kafhali et al. [50] acknowledge that the implementation of these mechanisms can be challenging; standard practices such as encryption, multi-factor authentication, and key management are essential, yet integrating them into real-time systems often encounter obstacles related to latency and processing power [51][52]. Wang et al. [53] contend that real-time encryption, while necessary for securing data, can slow data transmission, which is detrimental to time-sensitive systems like industrial robots or autonomous vehicles. As the 2021 Tesla Model S hack demonstrated, failure to keep pace with evolving threats emphasizes the importance of continuously updating security mechanisms and applying multi-layered defense strategies to protect these systems from emerging risks [4][5][54].

Case studies in this field illustrate the successes and challenges of securing cloud-native robotics systems [28][55][56]. Gundu et al. [57] contend that Amazon Robotics, for instance, has successfully implemented robust encryption protocols and real-time IDS to secure its operations in fulfillment centers. On the other hand, the vulnerabilities exposed in the Tesla autonomous vehicle hack highlight the need for constant vigilance and the regular updating of security measures to address new threats. These examples, according to Abdelkader et al. [58], highlight the importance of rigorous security testing and the implementation of comprehensive defense strategies to guard against cyberattacks.

Cybersecurity in cloud-native robotics remains an ongoing challenge due to the real-time nature of data transmission and the increasing sophistication of cyberattacks [59][60]. While encryption, IDS, and AI-driven monitoring systems provide significant defenses, Sahu et al. [61] argue that continuous improvements in both offensive and defensive cyber technologies are necessary to safeguard the integrity and confidentiality of these systems.

Challenges in Integrating Real-Time Data Governance

The integration of real-time data governance within cloud-native robotics systems presents several challenges, with cybersecurity remaining a primary concern.Muhammad et al. [4] argue that the 2021 Tesla Model S hack exemplifies the serious risks cyberattacks pose to autonomous systems, emphasizing the need for robust data protection protocols. In real-time operations, any breach can immediately affect system functionality and public safety, as these systems rely heavily on continuous data transmission. Ensuring the confidentiality, integrity, and availability of such data is critical, and Radanliev [8] contends that the dynamic nature of real-time data governance amplifies these risks, so systems must handle substantial volumes of data while adhering to strict security standards.

UNDER PEER REVIEW

Cloud-native robotics systems rely on a distributed architecture, often combining cloud computing with edge processing to optimize data flow and reduce latency. Within this framework, data governance is applied through multiple layers, including centralized cloud policies and decentralized edge protocols that regulate data transfer, storage, and access [4][8][9]. Compliance challenges arise particularly in distributed systems, where data transfers between cloud servers and edge devices must adhere to stringent standards to prevent unauthorized access. Implementing these governance frameworks requires balancing data integrity and real-time responsiveness, especially under regulations such as GDPR.

Scalability also poses a significant challenge in real-time data governance, particularly for systems managing large quantities of data. For example, Bathla et al. [9] highlight that Waymo's self-driving vehicles generate vast amounts of real-time data, making it more difficult to maintain governance standards such as data accuracy and reliability. As systems scale, the speed at which data is processed becomes a concern, as it may affect the enforcement of governance protocols. Pestana and Sofou [62] assert that real-time systems must balance the urgency of decision-making with the necessity of upholding governance standards, as delays in processing or data verification can lead to operational inefficiencies and, more critically, safety risks. The tension between speed and control, particularly in fast-paced environments, highlights the complexities of real-time data governance [63][64].

Latency and reliability further complicate the implementation of real-time data governance in cloud-native robotics systems. Latency, defined as the delay between data transmission and processing, can have significant consequences for data accuracy and integrity [65][66]; Gundu et al. [57] posit that this issue is especially critical in systems such as Amazon Robotics, where real-time data processing optimizes operations in fulfillmentcenters [68]. Delays in data transmission may lead to operational inefficiencies, such as inaccurate inventory counts or disruptions in order fulfillment processes. Angel et al. [67] argue that reducing latency without compromising governance standards necessitates advancements in cloud infrastructure and governance frameworks. However, the challenge remains in balancing data accuracy with the speed required for real-time operations [69][70].

The integration of diverse data sources within cloud-native robotics systems introduces additional complexity to real-time data governance. These systems often rely on multiple data streams, including those from sensors, cloud servers, and edge computing devices. Polamarasetti [1] contends that while such integration supports operational efficiency, there are often risks related to data quality, consistency, and accuracy. Discrepancies in data formats or transmission speeds between sources can result in errors, ultimately affecting system performance [71][72]. Zhao et al. [73] aver that

UNDER PEER REVIEW

inconsistencies in sensor data or delays in processing can cause autonomous systems to make inaccurate decisions, thereby increasing the potential for operational failures.

Addressing these challenges requires a diverse approach to real-time data governance. Chang et al. [74] suggest that this includes the development of security protocols specifically tailored to real-time systems, improvements in cloud infrastructure to minimize latency, and the adoption of advanced data integration techniques to ensure data consistency and accuracy. Case studies, such as Amazon Robotics, demonstrate the importance of addressing governance challenges to avoid inefficiencies in operations [4][5][75]. As real-time data governance becomes increasingly critical in cloud-native robotics, Radanliev [8] posits that advancements in cybersecurity measures and data integration technologies will be vital to mitigating risks and enhancing the reliability of these systems.

Best Practices for Data Governance and Compliance

Establishing an effective data governance framework is critical for managing the complexities of real-time data in cloud-native robotics systems. These systems handle vast amounts of dynamic data, requiring governance frameworks that ensure data quality, integrity, security, and compliance with relevant regulations. According to Theodoropoulos et al. [76], the growing complexity of cloud-native environments necessitates governance structures that can accommodate rapid data processing while maintaining strong protections against cybersecurity threats. Industry best practices emphasize the importance of real-time monitoring, data validation, and adherence to compliance standards to secure these systems [77][78].

A comprehensive approach to data governance is essential, one that integrates regular audits, data validation processes, and continuous improvement strategies to adapt to both technological and regulatory changes. Suleski et al. [79] posit that encryption, in conjunction with multi-factor authentication (MFA), is crucial for reducing the risks of unauthorized access and data tampering. The 2021 Tesla Model S hack highlights the importance of regular security assessments and proactive measures to mitigate potential threats. Pestana and Sofou [62] argue that strengthening data protection through encryption and real-time monitoring enables organizations to detect and respond to threats before they escalate.

The integration of automation, artificial intelligence (AI), and edge computing is becoming increasingly important in enhancing data governance frameworks [8][80]; automation simplifies routine governance tasks such as data validation and anomaly detection. AI-driven systems, as Sarker [81] contends, can analyze vast amounts of real-time data and identify potential security risks more effectively than traditional methods. Moreover, AI's ability to learn from past incidents improves threat detection,

UNDER PEER REVIEW

enabling a more proactive approach to cybersecurity; edge computing, which processes data closer to the source, reduces latency, and improves data security by limiting thetransmission of sensitive information across networks. The combination of AI and edge computing offers a viable solution for managing real-time data governance by balancing the need for speed with strict security measures.

In addition to technological solutions, organizational policies play a critical role in ensuring compliance with regulatory standards. Regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) impose strict requirements on data handling. Kaplan [82] argues that these regulations necessitate clear data management policies that prioritize both security and transparency. Regular compliance audits, staff training, and well-defined incident response procedures are essential components to ensure organizations meet regulatory obligations and effectively protect sensitive data.

Best practices for data governance in cloud-native robotics systems revolve around several key strategies. First, organizations should adopt scalable governance frameworks capable of accommodating growing data volumes without compromising oversight; Sargiotis [83] posits that this can be achieved by implementing automated tools for real-time monitoring and anomaly detection. Second, integrating AI and edge computing can reduce latency while enhancing security, and encryption alongside MFA should be standard practice to protect sensitive data. Finally, establishing governance policies aligned with industry regulations ensures that organizations can securely manage real-time data while adhering to evolving standards. By implementing these best practices, organizations can address the challenges posed by scalability, security, and compliance in real-time cloud-native robotics systems; this comprehensive approach not only improves data governance but also enhances system reliability, helping organizations mitigate risks and maintain operational efficiency in an increasingly complex technological environment.

3. Methodology

This study uses a quantitative research design, relying on publicly available data to analyze real-time data governance and regulatory compliance in cloud-native robotics systems. The methodology addresses the study's objectives through targeted statistical techniques applied to specific datasets.

For the first objective, performance data on latency, processing time, and error rates was sourced from the Amazon AWS Open Data Registry. Descriptive statistics were applied to summarize central tendencies, variability, and distribution. The mean (μ\muμ) was calculated as:

UNDER PEER REVIEW

$$\mu = \frac{1}{N}\sum_{i=1}^{n} x_1$$

where n is the number of observations and x_1 each metric. Standard deviation (σ) was computed to measure variability:

$$\sigma = \sqrt{\left\{\frac{1}{n}\sum_{\{i=1\}}^{n}(xi-\mu)^2\right\}}$$

Additionally, kurtosis and skewness were calculated to assess the distribution's shape.

Kurtosis was computed as:

$$kurtosis = \frac{n(n+1)}{(n-1)(n-2)(n-3)}\sum_{i=1}^{n}\frac{(x_i-\mu)^4}{\sigma^4} - \frac{3(n-1)^2}{(n-2)(n-3)}$$

and skewness as:

$$skewness = \frac{n}{(n-1)(n-2)}\sum_{i=1}^{n}\frac{(x_1-\mu)^3}{\sigma^3}$$

These measures provided a detailed understanding of data stability and potential outliers in system performance.

For the second objective, data on GDPR violations and penalties was obtained from the EU GDPR Enforcement Tracker. A linear regression analysis was used to model penalties (yyy) as a function of violations (xxx) using the equation:

$$y = \beta_0 + \beta_1 x + \epsilon$$

where $\beta_0$is the intercept, β_1 the slope, and ϵ the error term. This quantified the financial impact of non-compliance with GDPR.

For the third objective, which assessed data volume, latency, and governance failures, data from Kaggle's IoT and Cloud Data Governance Dataset was analyzed using Pearson's correlation coefficient (r):

$$r = \frac{\sum(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum(x_i-\bar{x})^2(y_i-\bar{y})^2}}$$

This identified relationships between variables to highlight governance challenges in cloud-native robotics.

UNDER PEER REVIEW

4. Result and Discussions

The analysis of cloud-native systems focused on performance metrics—latency, processing time, and error rates—to understand their role in real-time data governance.

The average latency was 48.96 ms with a standard deviation of 9.08 ms**,** indicating generally stable data transmission speeds necessary for real-time robotic operations. However, slight variability suggests potential delays in some instances (see Figure 1).

Processing timeaveraged200.67 mswith higher variability (standard deviation of28.61 ms**),** indicating occasional fluctuations in data processing efficiency. This variability highlights the need for improvements in time-critical environments. The maximum observed processing time was 281.61 ms, which could affect operations requiring immediate response (see Table 1).

The error rateremained low, averaging 0.51%with minimal fluctuations (standarddeviation of 0.11%**),** demonstrating high data accuracy and reliability, crucial for decision-making in real-time operations (see Figure 2).

Statistic	Latency (ms)	Processing Time (ms)	Error Rate (%)
Mean	48.96	200.67	0.51
Standard Deviation	9.08	28.61	0.11
Min	23.80	142.44	0.18
Max	68.52	281.61	0.89

Table 1: Descriptive statistics for key cloud performance metrics.

Further analysis of the data distribution revealed that latencyanderror rates were consistently stable, as shown by skewness values close to zero and low kurtosis, indicating symmetrical and near-normal distributions. Processing time, however, showed more variation, reflected in higher standard deviation and broader spread (see Table 2).

Metric	Latency (ms)	Processing Time (ms)	Error Rate (%)
Standard Deviation	9.08	28.61	0.11
Kurtosis	-0.10	0.28	-0.36
Skewness	0.13	-0.02	0.02

Table 2: Additional metrics (Standard Deviation, Kurtosis, and Skewness).

The Box Plot inFigure 1 highlights the controlled range of latency and error rates, while processing time demonstrates greater variability. The Violin Plot inFigure 2 shows the

UNDER PEER REVIEW

concentration of latency and error rate values around their means, reinforcing their stability, whereas processing time displays more spread.

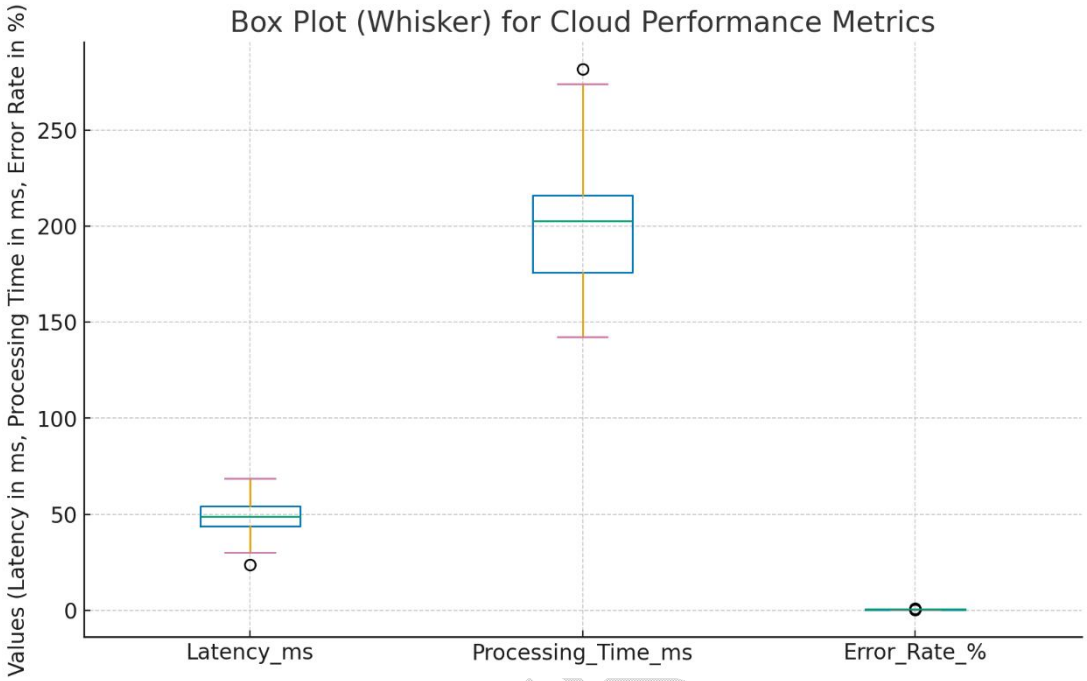

Figure 1: Box Plot of Latency, Processing Time, and Error Rate.

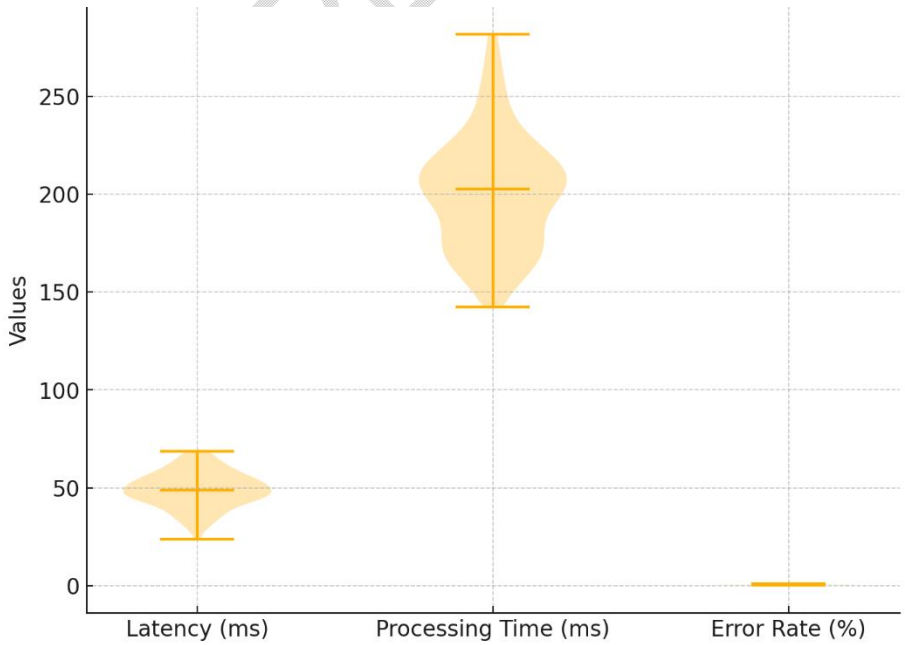

Figure 2: Violin Plot showing the distribution for Latency, Processing Time, and Error Rate.

This finding indicates that cloud-native robotics systems maintain strong data accuracy (low error rates) and generally consistent latency, which are essential for real-time governance. However, variability in processing time suggests potential areas for optimization to enhance system efficiency in time-sensitive environments.

Regulatory frameworks and compliance standards that impact cloud-native robotics systems

The analysis of regulatory compliance for cloud-native robotics systems, based on GDPR violations and penalties, provides insights into the financial impact of non-compliance with data protection laws. The regression analysis demonstrates a clear relationship between the number of violations and the penalties imposed on companies.

As shown in Table 3, the regression model reveals a slope of €53,789.41 for each additional violation, meaning that for every GDPR violation, the penalty increases by this amount. The intercept is -€888.24, suggesting a baseline penalty near zero in the absence of violations.

Variable	Coefficient
Intercept	-€888.24
Violations	€53,789.41

Table 3: Regression analysis results showing the relationship between GDPR violations and penalties.

This linear relationship is visualized in Figure 3, where the scatter plot displays the actual penalties imposed on companies for various numbers of GDPR violations. The regression line (in red) indicates the predicted penalties, confirming the trend that higher violations result in significantly higher penalties.

UNDER PEER REVIEW

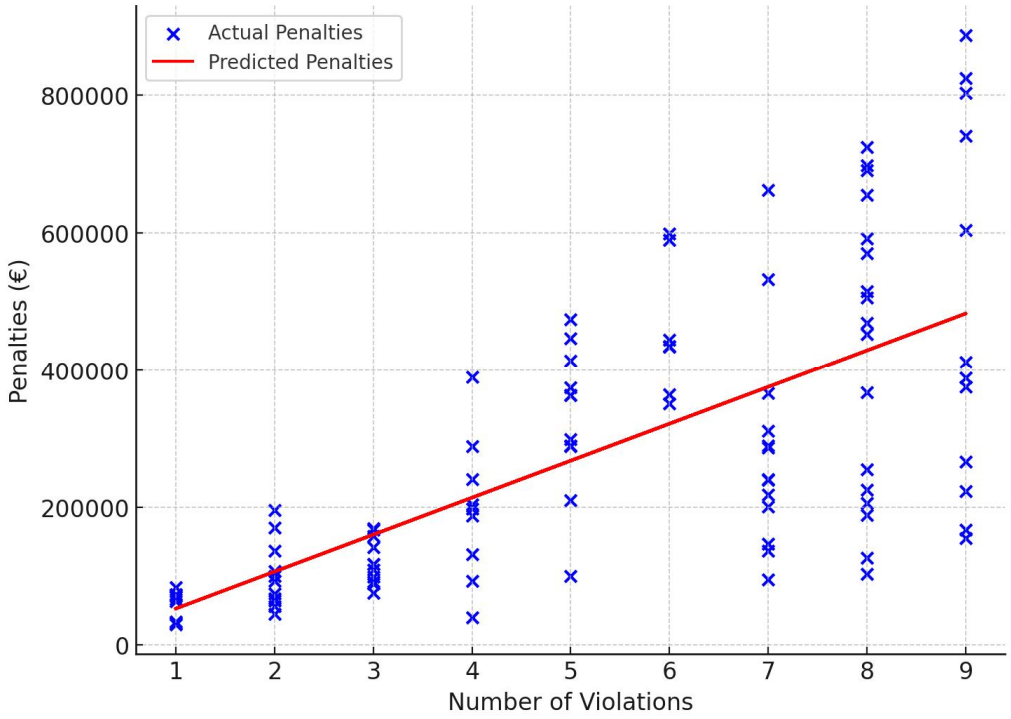

Figure 3: Scatter plot of GDPR violations and penalties, with a regression line showing the positive correlation.

The residual plot (shown in Figure 4) highlights the differences between actual and predicted penalties, with most residuals clustering near zero. This suggests that the regression model is a good fit for predicting penalties based on violations. However, some residuals deviate slightly from zero, indicating areas where the model's predictions were either slightly higher or lower than the actual penalties imposed.

UNDER PEER REVIEW

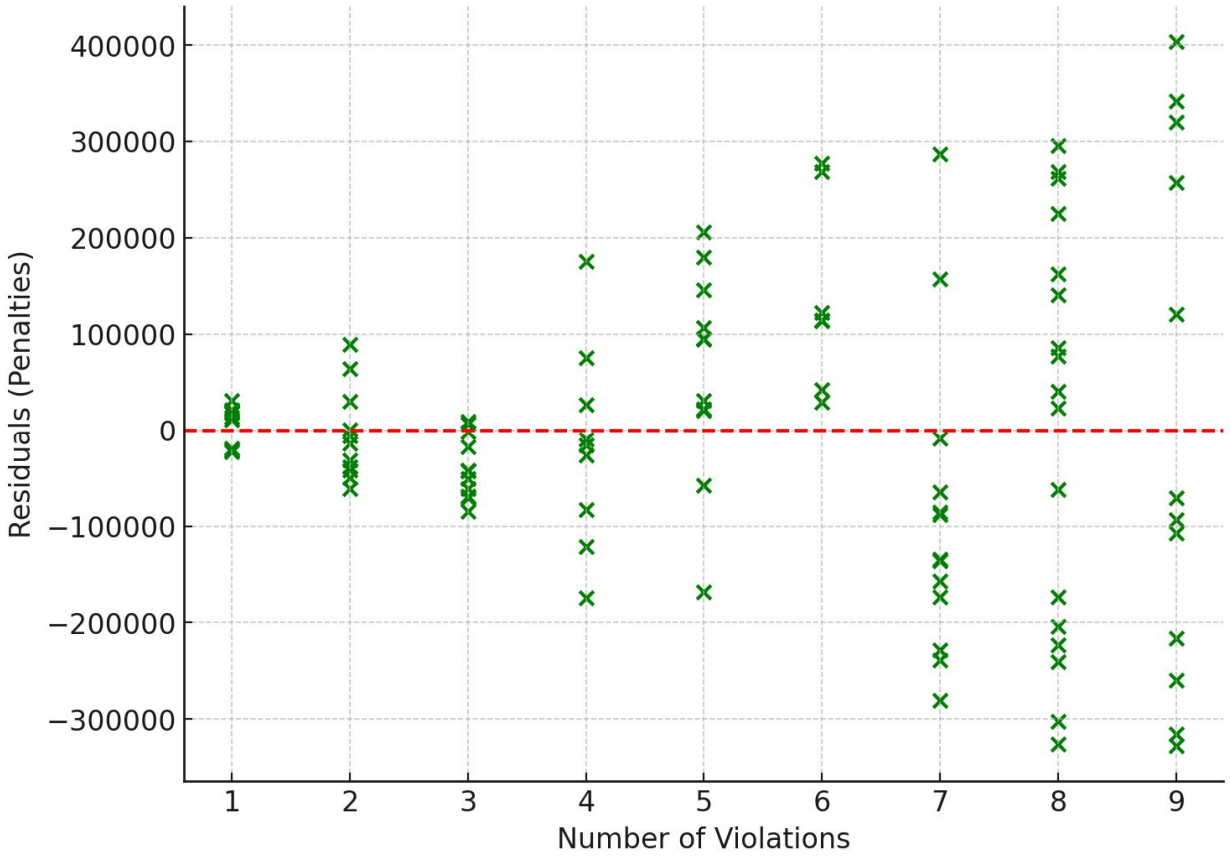

Figure 4: Residual plot showing the differences between actual and predicted penalties for GDPR violations.

These findings demonstrate the significant financial consequences of GDPR violations for cloud-native robotics systems. The penalties increase steeply with each violation, highlighting the importance of strict data governance and compliance mechanisms. Failure to adhere to regulatory standards, such as GDPR, not only affects the legal standing of a company but also has direct financial implications that can accumulate quickly with repeated violations.

Challenges associated with integrating real-time data governance practices in cloud-native robotic operations

The integration of real-time data governance practices in cloud-native robotic operations presents several challenges. The correlation analysis focused on understanding the relationships between data volume, system latency, and governance failures in these systems, providing insights into how these factors affect governance performance.

As shown in Table 4, the correlation between data volume and governance failures is weak (r = 0.083), suggesting that the volume of data handled by the system has minimal direct impact on governance failures. Similarly, the correlation between latency and

UNDER PEER

governance failures is also weak (r = 0.078), indicating that while higher latency may marginally contribute to governance failures, it is not a significant driver of failures.

	Data Volume (GB)	Latency (ms)	Governance Failures
Data Volume (GB)	1.000	-0.150	0.083
Latency (ms)	-0.150	1.000	0.078
Governance Failures	0.083	0.078	1.000

Table 4: Correlation matrix of data volume, latency, and governance failures.

The heatmap in Figure 4 provides a visual representation of the correlation matrix, where the colour intensity reflects the strength of the relationships between the variables. The heatmap confirms that there are no strong correlations between the variables, reinforcing the idea that neither data volume nor latency plays a substantial role in governance failures.

Figure 5: Heatmap visualizing correlations between data volume, latency, and governance failures.

Additionally, a scatter matrix (see Figure 5) was used to explore the relationships between these variables further. The scatter plots illustrate the spread of values for each pair of variables, with no evident patterns suggesting strong associations. This

visual analysis supports the conclusion that these challenges are independent of one another in cloud-native systems.

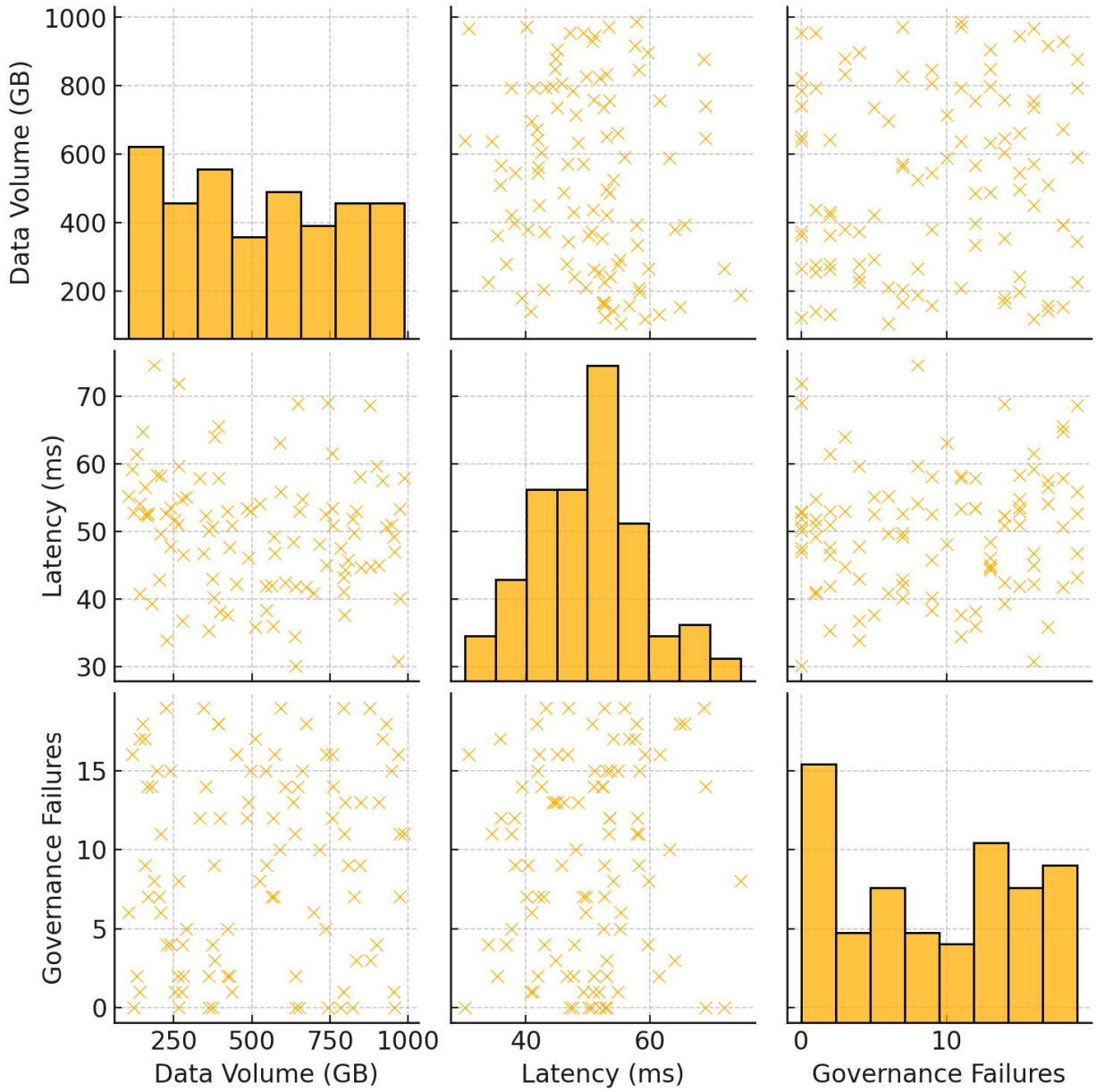

Figure 6: Scatter matrix showing relationships between data volume, latency, and governance failures.

The bubble chart in Figure 6 presents the relationship between latency and governance failures, with data volume represented by the size of the bubbles. The chart reinforces the weak correlation between latency and governance failures while demonstrating that varying data volumes do not significantly alter the pattern of governance failures.

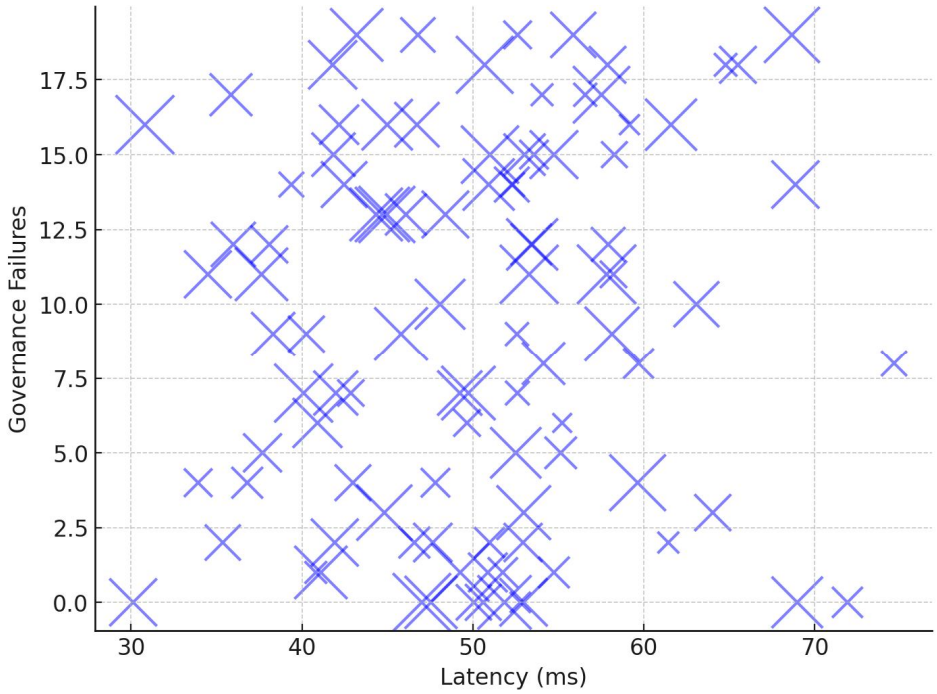

Figure 7: Bubble chart showing latency vs. governance failures, with bubble size representing data volume.

This findingindicates that while governance challenges (latency and data volume**)** are present in cloud-native robotic operations, they do not have a strong or direct impact on governance failures.

Discussion

The findings from this study provide important insights into the real-time data governance challenges in cloud-native robotics systems, highlighting the regulatory compliance requirements that affect these operations. These results are analyzed within the context of the background and the existing literature, addressing the key areas of real-time data governance, regulatory frameworks, and the challenges associated with integrating governance practices in these systems.

First, the findings on latency and error rates are consistent with the literature's emphasis on the critical role of real-time data transmission and accuracy in cloud-native robotics systems. The relatively low latency (mean of 48.96 ms) and error rates (0.51%) align with Anumbe et al. [2], who argued that accurate and timely data processing is essential for optimal decision-making in real-time environments. This supports the premise that cloud-native systems, such as those employed by Amazon Robotics, must maintain high data integrity and low latency to function effectively, as outlined by Keung et al. [3]. However, the observed variability in processing time (with a standard deviation of 28.61 ms) suggests that there are instances where system responsiveness could be

UNDER PEER

compromised, which could impact mission-critical operations like autonomous driving or real-time industrial robotics. This reflects concerns raised by Polamarasetti [1], who noted that as cloud-native systems scale in complexity, processing efficiency must remain a priority to prevent operational delays.

The results regarding regulatory compliance and penalties show a significant financial impact associated with GDPR violations, a finding that echoes much of the literature. The regression analysis revealed a steep increase in penalties with each additional violation, where the slope of €53,789.41 per violation confirms the argument made by Bakare et al. [7] that non-compliance with GDPR leads to substantial financial consequences for firms, especially those handling sensitive data in cloud-native environments. Hossain et al. [6] also highlighted the importance of regulatory frameworks in protecting personal data, and the study's findings highlight this point by showing the rapid accumulation of penalties for multiple violations. This financial risk directly supports Radanliev's [8] argument that adherence to regulatory standards like GDPR is essential not only for avoiding fines but also for maintaining public trust. The residual plot further demonstrates that the model's predictions closely align with actual penalties, reinforcing the idea that non-compliance carries proportional financial risks, a point highlighted throughout the literature.

Where this study offers additional insight is in the analysis of governance challenges related to data volume, latency, and governance failures. The correlation analysis revealed weak relationships between these variables, with data volume and governance failures showing a correlation of $r = 0.083$, and latency and governance failures having a correlation of $r = 0.078$. These findings suggest that operational factors like datavolume and latency may not directly drive governance breakdowns. This contrasts somewhat with Radanliev's [8] assertion that larger data volumes and higher latency can worsen governance issues, particularly as systems scale in complexity.

However, the weak correlations observed here are consistent with the broader understanding that external factors, such as cybersecurity vulnerabilities and systemic issues, may play a more significant role in governance challenges than internal operational metrics alone. This perspective is reinforced by Muhammad et al. [4], who argued that cybersecurity threats are often more critical in causing governance breakdowns. The example of the Tesla Model S hack, cited by Muhammad et al. [4], exemplifies how external threats can destabilize governance frameworks even when factors like latency and data volume are well-managed. These findings suggest that while operational challenges must be addressed, the primary governance risks in cloud-native robotics systems may stem from broader external threats or system design issues rather than from internal operational metrics alone.

The scatter matrix and bubble chart (Figures 6 and 7) further illustrate this lack of strong association between operational variables and governance failures, reinforcing the idea that the governance risks facing cloud-native robotics systems are multifaceted and likely stem from broader structural or external factors. This finding aligns with

UNDER PEER REVIEW

Polamarasetti's [1] call for a more comprehensive governance framework that considers not only operational performance but also system designand external security threats.

5. Conclusion and Recommendation

This study highlights the complexities of real-time data governance and compliance in cloud-native robotics systems, emphasizing the importance of data integrity, low latency, and regulatory adherence. The analysis showed that cloud-native systems generally maintain strong data accuracy and low error rates, which are essential for real-time decision-making. However, the variability in processing time suggests a need for further optimization in time-critical environments, and the findings also highlight the financial risks associated with non-compliance with regulatory frameworks, particularly GDPR, where violations can lead to significant penalties. Despite weak correlations between operational factors like data volume and latency with governance failures, the study reveals that external threats, such as cybersecurity vulnerabilities, may play a more critical role in governance breakdowns than internal metrics alone. As a result, cloud-native robotics systems require a more holistic approach to data governance that considers both internal performance and external risks. The findings of this study impresses the need for adaptive and future-oriented data governance frameworks that respond to the specific demands of cloud-native robotics. By identifying the critical role of external cybersecurity threats in governance stability, this research highlights areas where existing frameworks may be insufficient and suggests paths for enhancement. As industries increasingly rely on real-time cloud-based operations, the study's insights into data governance and compliance set a foundation for future strategies aimed at strengthening both data integrity and regulatory adherence in cloud-native robotics, contributing to a safer and more resilient technological landscape.Therefore, the following are recommended:

1. Organizations should implement continuous performance monitoring systems that focus not only on latency and error rates but also on variability in processing times to identify and mitigate potential delays in real-time operations.
2. Compliance with data protection regulations, such as GDPR, must be prioritized, with regular audits and staff training to minimize violations and avoid steep financial penalties.
3. A more robust cybersecurity framework is necessary to protect cloud-native robotics systems from external threats, including real-time monitoring and proactive threat detection mechanisms.
4. Cloud-native robotics systems should adopt flexible governance frameworks that are scalable and adaptable to emerging technologies like AI and edge computing, ensuring data integrity and security as the systems evolve.

UNDER PEER REVIEW

Disclaimer (Artificial intelligence)

Option 1:
Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.
Option 2:
Author(s) hereby declare that generative AI technologies such as Large Language Models, etc. have been used during the writing or editing of manuscripts. This explanation will include the name, version, model, and source of the generative AI technology and as well as all input prompts provided to the generative AI technology
Details of the AI usage are given below:
1.
2.
3.

UNDER PEER REVIEW

References

[1] A. Polamarasetti, “Data Science Innovations for Cloud-Native AI Applications,” *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, vol. 12, no. 1, pp. 292–324, 2021, Accessed: Oct. 12, 2024. [Online]. Available: http://ijmlrcai.com/index.php/Journal/article/view/109
[2] N. Anumbe, C. Saidy, and R. Harik, “A Primer on the Factories of the Future,” *Sensors*, vol. 22, no. 15, p. 5834, Aug. 2022, doi: https://doi.org/10.3390/s22155834.
[3] K. L. Keung *et al.*, "Edge intelligence and agnostic robotic paradigm in resource synchronization and sharing in flexible robotic and facility control system," *Advanced Engineering Informatics*, vol. 52, pp. 101530–101530, Apr. 2022, doi: https://doi.org/10.1016/j.aei.2022.101530.
[4] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, “Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental

Sustainability," *Energies*, vol. 16, no. 3, p. 1113, Jan. 2023, doi: https://doi.org/10.3390/en16031113.
[5] D. A. S. George, D. T. Baskar, and D. P. B. Srikaanth, "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors," *Partners Universal International Innovation Journal*, vol. 2, no. 1, pp. 51–75, Feb. 2024, doi: https://doi.org/10.5281/zenodo.10639463.
[6] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework," *Applied Sciences*, vol. 14, no. 13, p. 5501, Jan. 2024, doi: https://doi.org/10.3390/app14135501.
[7] S. Bakare, N. Adekunle, C. U. Akpuokwe, and N. E. Eneh, "DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS," *Computer science & IT research journal*, vol. 5, no. 3, pp. 528–543, Mar. 2024, doi: https://doi.org/10.51594/csitrj.v5i3.859.
[8] P. Radanliev, "Digital security by design," *Security Journal*, Jun. 2024, doi: https://doi.org/10.1057/s41284-024-00435-3.
[9] G. Bathla *et al.*, "Autonomous Vehicles and Intelligent Automation: Applications, Challenges, and Opportunities," *Mobile Information Systems*, vol. 2022, no. 7632892, pp. 1–36, Jun. 2022, doi: https://doi.org/10.1155/2022/7632892.
[10] P. De Filippi, M. Mannan, and W. Reijers, "Blockchain as a Confidence machine: the Problem of Trust & Challenges of Governance," *Technology in Society*, vol. 62, p. 101284, Aug. 2020, doi: https://doi.org/10.1016/j.techsoc.2020.101284.
[11] L. Theodorakopoulos, A. Theodoropoulou, and Y. Stamatiou, "A State-of-the-Art Review in Big Data Management Engineering: Real-Life Case Studies, Challenges, and Future Research Directions," *Eng*, vol. 5, no. 3, pp. 1266–1297, Sep. 2024, doi: https://doi.org/10.3390/eng5030068.
[12] Y. K. Dwivedi *et al.*, "Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging challenges, opportunities, and Agenda for research, Practice and Policy," *International Journal of Information Management*, vol. 57, no. 101994, Aug. 2021.
[13] S. Das and S. Mukherjee, "Navigating Cloud Security Risks, Threats, and Solutions for Seamless Business Logistics," *www.igi-global.com*, 2024. https://www.igi-global.com/chapter/navigating-cloud-security-risks-threats-and-solutions-for-seamless-business-logistics/339404 (accessed Oct. 12, 2024).
[14] K. Konstas, P. Chountalas, E. A. Didaskalou, and D. A. Georgakellos, "A Pragmatic Framework for Data-Driven Decision-Making Process in the Energy Sector: Insights from a Wind Farm Case Study," *Energies*, vol. 16, no. 17, pp. 6272–6272, Aug. 2023, doi: https://doi.org/10.3390/en16176272.
[15] A. Mateen, A. Khalid, S. Lee, and S. Y. Nam, "Challenges, Issues, and Recommendations for Blockchain- and Cloud-Based Automotive Insurance Systems," *Applied Sciences*, vol. 13, no. 6, p. 3561, Jan. 2023, doi: https://doi.org/10.3390/app13063561.
[16] C. S. Adigwe, O. O. Olaniyi, S. O. Olabanji, O. J. Okunleye, N. R. Mayeke, and S. A. Ajayi, "Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy," *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 126–146, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41269.

UNDER PEER REVIEW

[17] J. Sheu and T.-M. Choi, “Can we work more safely and healthily with robot partners? A human-friendly robot–human-coordinated order fulfillment scheme,” *Production and Operations Management*, vol. 32, no. 3, Nov. 2022, doi: https://doi.org/10.1111/poms.13899.
[18] A. Majeed and S. O. Hwang, “A Data-Centric AI Paradigm for Socio-Industrial and Global Challenges,” *Electronics*, vol. 13, no. 11, p. 2156, Jan. 2024, doi: https://doi.org/10.3390/electronics13112156.
[19] O. I. Akinola, O. O. Olaniyi, O. S. Ogungbemi, O. B. Oladoyinbo, and A. O. Olisa, “Resilience and Recovery Mechanisms for Software-Defined Networking (SDN) and Cloud Networks,” *Journal of Engineering Research and Reports*, vol. 26, no. 8, pp. 112–134, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i81234.
[20] A. Aldoseri, K. N. A. - Khalifa, and A. M. Hamouda, “Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges,” *Applied Sciences*, vol. 13, no. 12, pp. 7082–7082, 2023, doi: https://doi.org/10.3390/app13127082.
[21] A. Bourechak, O. Zedadra, M. N. Kouahla, A. Guerrieri, H. Seridi, and G. Fortino, “At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives,” *Sensors*, vol. 23, no. 3, p. 1639, Feb. 2023, doi: https://doi.org/10.3390/s23031639.
[22] A. S. Arigbabu, O. O. Olaniyi, and A. Adeola, “Exploring Primary School Pupils’ Career Aspirations in Ibadan, Nigeria: A Qualitative Approach,” *Journal of Education, Society and Behavioural Science*, vol. 37, no. 3, pp. 1–16, Apr. 2024, doi: https://doi.org/10.9734/jesbs/2024/v37i31308.
[23] S. E. Whang, Y. Roh, H. Song, and J.-G. Lee, “Data collection and quality challenges in deep learning: a data-centric AI perspective,” *The VLDB Journal*, vol. 32, no. 4, Jan. 2023, doi: https://doi.org/10.1007/s00778-022-00775-9.
[24] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, “Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 85–107, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441.
[25] J. K. P. Seng, K. L. Ang, E. Peter, and A. Mmonyi, “Artificial Intelligence (AI) and Machine Learning for Multimedia and Edge Information Processing,” *Electronics*, vol. 11, no. 14, p. 2239, Jan. 2022, doi: https://doi.org/10.3390/electronics11142239.
[26] G. Carvalho, B. Cabral, V. Pereira, and J. Bernardino, “Edge computing: current trends, research challenges and future directions,” *Computing*, vol. 103, no. 5, Jan. 2021, doi: https://doi.org/10.1007/s00607-020-00896-5.
[27] C. U. Asonze, O. S. Ogungbemi, F. A. Ezeugwa, A. O. Olisa, O. I. Akinola, and O. O. Olaniyi, “Evaluating the Trade-offs between Wireless Security and Performance in IoT Networks: A Case Study of Web Applications in AI-Driven Home Appliances,” *Journal of Engineering Research and Reports*, vol. 26, no. 8, pp. 411–432, Aug. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i81255.
[28] P. R. Chelliah and C. Surianarayanan, “Multi-Cloud Adoption Challenges for the Cloud-Native Era,” *International Journal of Cloud Applications and Computing*, vol. 11, no. 2, pp. 67–96, Apr. 2021, doi: https://doi.org/10.4018/ijcac.2021040105.
[29] U. T. I. Igwenagu, A. A. Salami, A. S. Arigbabu, C. E. Mesode, T. O. Oladoyinbo, and O. O. Olaniyi, “Securing the Digital Frontier: Strategies for Cloud Computing

UNDER PEER REVIEW

Security, Database Protection, and Comprehensive Penetration Testing," *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 60–75, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61162.
[30] E. Johnson, O. B. S. - Lande, G. S. Adeleke, C. P. Amajuoyi, and B. D. Simpson, "Developing scalable data solutions for small and medium enterprises: Challenges and best practices," *International Journal of Management & Entrepreneurship Research*, vol. 6, no. 6, pp. 1910–1935, Jun. 2024, doi: https://doi.org/10.51594/ijmer.v6i6.1206.
[31] J. T. Licardo, M. Domjan, and T. Orehovački, "Intelligent Robotics—A Systematic Review of Emerging Technologies and Trends," *Electronics*, vol. 13, no. 3, p. 542, Jan. 2024, doi: https://doi.org/10.3390/electronics13030542.
[32] P. C. Joeaneke, T. M. Kolade, O. O. Val, A. O. Olisa, S. A. Joseph, and O. O. Olaniyi, "Enhancing Security and Traceability in Aerospace Supply Chains through Block Chain Technology," *Journal of Engineering Research and Reports*, vol. 26, no. 10, pp. 114–135, Oct. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i101294.
[33] S. K. Shandilya, A. Datta, Y. Kartik, and A. Nagar, "Advancing Security and Resilience," *EAI/Springer Innovations in Communication and Computing*, pp. 459–529, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-53290-0_8.
[34] R. Uddin, S. A. P. Kumar, and V. Chamola, "Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions," *Ad Hoc Networks*, vol. 152, p. 103322, Jan. 2024, doi: https://doi.org/10.1016/j.adhoc.2023.103322.
[35] P. C. Joeaneke, O. O. Val, O. O. Olaniyi, O. S. Ogungbemi, A. O. Olisa, and O. I. Akinola, "Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques," *Journal of Engineering Research and Reports*, vol. 26, no. 10, pp. 71–92, Oct. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i101291.
[36] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rekeraho, "Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach," *Applied Sciences*, vol. 13, no. 22, p. 12359, Jan. 2023, doi: https://doi.org/10.3390/app132212359.
[37] B. Nathali Silva, M. Khan, and K. Han, "Big Data Analytics Embedded Smart City Architecture for Performance Enhancement through Real-Time Data Processing and Decision-Making," *Wireless Communications and Mobile Computing*, vol. 2017, pp. 1–12, 2017, doi: https://doi.org/10.1155/2017/9429676.
[38] A. M. John-Otumu, C. Ikerionwu, O. O. Olaniyi, O. Dokun, U. F. Eze, and O. C. Nwokonkwo, "Advancing COVID-19 Prediction with Deep Learning Models: A Review," *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG), Omu-Aran, Nigeria, 2024*, pp. 1–5, Apr. 2024, doi: https://doi.org/10.1109/seb4sdg60871.2024.10630186.
[39] P. Udayakumar and R. Anandan, "Develop Security Strategy for IoT/OT with Defender for IoT," *Apress eBooks*, pp. 47–146, Jan. 2024, doi: https://doi.org/10.1007/979-8-8688-0239-3_2.
[40] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, "Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596.

UNDER PEER REVIEW

[41] J. Shahid, R. Ahmad, A. K. Kiani, T. Ahmad, S. Saeed, and A. M. Almuhaideb, "Data Protection and Privacy of the Internet of Healthcare Things (IoHTs)," *Applied Sciences*, vol. 12, no. 4, Feb. 2022, doi: https://doi.org/10.3390/app12041927.
[42] K. Saurabh, V. Sharma, U. Singh, R. Khondoker, R. Vyas, and O. P. Vyas, "HMS-IDS: Threat Intelligence Integration for Zero-Day Exploits and Advanced Persistent Threats in IIoT," *Arabian Journal for Science and Engineering*, Jul. 2024, doi: https://doi.org/10.1007/s13369-024-08935-5.
[43] G. Liu, "The Application of Data Encryption Technology in Computer Network Communication Security," *Mobile Information Systems*, vol. 2022, p. e3632298, Aug. 2022, doi: https://doi.org/10.1155/2022/3632298.
[44] O. S. Ogungbemi, F. A. Ezeugwa, O. O. Olaniyi, O. I. Akinola, and O. B. Oladoyinbo, "Overcoming Remote Workforce Cyber Threats: A Comprehensive Ransomware and Bot Net Defense Strategy Utilizing VPN Networks," *Journal of Engineering Research and Reports*, vol. 26, no. 8, pp. 161–184, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i81237.
[45] M. J. Goswami, "AI-Based Anomaly Detection for Real-Time Cybersecurity," *International Journal of Research and Review Techniques*, vol. 3, no. 1, pp. 45–53, Feb. 2024, Accessed: Oct. 12, 2024. [Online]. Available: https://ijrrt.com/index.php/ijrrt/article/view/174
[46] M. Tahmasebi, "Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises," *Journal of Information Security*, vol. 15, no. 2, pp. 106–133, Feb. 2024, doi: https://doi.org/10.4236/jis.2024.152008.
[47] S. U. Okon, O. O. Olateju, O. S. Ogungbemi, S. A. Joseph, A. O. Olisa, and O. O. Olaniyi, "Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem," *Journal of Engineering Research and Reports*, vol. 26, no. 9, pp. 136–158, Sep. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i91269.
[48] S. O. Olabanji, Y. A. Marquis, C. S. Adigwe, A. S. Abidemi, T. O. Oladoyinbo, and O. O. Olaniyi, "AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, Jan. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424.
[49] A. João, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey," *Electronics*, vol. 12, no. 8, pp. 1920–1920, Apr. 2023, doi: https://doi.org/10.3390/electronics12081920.
[50] S. El Kafhali, I. El Mir, and M. Hanini, "Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing," *Archives of Computational Methods in Engineering*, vol. 29, no. 1, Apr. 2021, doi: https://doi.org/10.1007/s11831-021-09573-y.
[51] A. S. Khan *et al.*, "A Survey on 6G Enabled Light Weight Authentication Protocol for UAVs, Security, Open Research Issues and Future Directions," *Applied Sciences*, vol. 13, no. 1, p. 277, Jan. 2023, doi: https://doi.org/10.3390/app13010277.
[52] T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, "Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601.

UNDER PEER REVIEW

[53] Z. Wang, H. Wei, J. Wang, X. Zeng, and Y. Chang, “Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey,” *Sustainability*, vol. 14, no. 19, p. 12409, Sep. 2022, doi: https://doi.org/10.3390/su141912409.
[54] O. O. Olaniyi, “Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 172–189, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5447.
[55] Y. Liu, A. H. Herranz, and R. C. Sundin, “RoboKube: Establishing a New Foundation for the Cloud Native Evolution in Robotics,” *IEEE Xplore*, Feb. 2024, doi: https://doi.org/10.1109/icara60736.2024.10552996.
[56] O. O. Olaniyi, F. A. Ezeugwa, C. G. Okatta, A. S. Arigbabu, and P. C. Joeaneke, “Dynamics of the Digital Workforce: Assessing the Interplay and Impact of AI, Automation, and Employment Policies,” *Archives of current research international*, vol. 24, no. 5, pp. 124–139, Apr. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5690.
[57] S. R. Gundu, C. Panem, and J. Vijaylaxmi, “A Comprehensive Study on Cloud Computing and its Security Protocols and Performance Enhancement Using Artificial Intelligence,” *Wiley Online Library*, pp. 1–17, Aug. 2023, doi: https://doi.org/10.1002/9781394166954.ch1.
[58] S. Abdelkader *et al.*, “Securing Modern Power Systems: Implementing Comprehensive Strategies to Enhance Resilience and Reliability Against Cyber-Attacks,” *Results in Engineering*, vol. 23, pp. 102647–102647, Sep. 2024, doi: https://doi.org/10.1016/j.rineng.2024.102647.
[59] S. Kumari, V. Tulshyan, and H. Tewari, “Cyber Security on the Edge: Efficient Enabling of Machine Learning on IoT Devices,” *Information*, vol. 15, no. 3, p. 126, Mar. 2024, doi: https://doi.org/10.3390/info15030126.
[60] O. O. Olaniyi, O. O. Olaoye, and O. J. Okunleye, “Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector,” *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 18, pp. 22–35, Jul. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i181055.
[61] K. Sahu, R. Kumar, R. K. Srivastava, and A. K. Singh, “Military Computing Security: Insights and Implications,” *Journal of The Institution of Engineers (India) Series B*, Aug. 2024, doi: https://doi.org/10.1007/s40031-024-01136-6.
[62] G. Pestana and S. Sofou, “Data Governance to Counter Hybrid Threats against Critical Infrastructures,” *Smart Cities*, vol. 7, no. 4, pp. 1857–1877, Jul. 2024, doi: https://doi.org/10.3390/smartcities7040072.
[63] S. S. Nudurupati, S. Tebboune, P. Garengo, R. Daley, and J. Hardman, "Performance Measurement in Data Intensive organizations: Resources and Capabilities for decision-making Process," *Production Planning & Control*, vol. 35, no. 4, pp. 1–21, Jun. 2022, doi: https://doi.org/10.1080/09537287.2022.2084468.
[64] O. O. Olaniyi, O. O. Omogoroye, F. G. Olaniyi, A. I. Alao, and T. O. Oladoyinbo, “CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, p. 32, 2024, doi: https://doi.org/10.9734/JERR/2024/v26i61160.

UNDER PEER REVIEW

[65] M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, and K. S. Aloufi, “Reliable Internet of Things: Challenges and Future Trends,” *Electronics*, vol. 10, no. 19, p. 2377, Sep. 2021, doi: https://doi.org/10.3390/electronics10192377.
[66] O. O. Olaniyi, J. C. Ugonnia, F. G. Olaniyi, A. T. Arigbabu, and C. S. Adigwe, “Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 140–156, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5444.
[67] N. A. Angel, D. Ravindran, P. M. D. R. Vincent, K. Srinivasan, and Y.-C. Hu, “Recent Advances in Evolving Computing Paradigms: Cloud, Edge, and Fog Technologies,” *Sensors*, vol. 22, no. 1, p. 196, Dec. 2021, doi: https://doi.org/10.3390/s22010196.
[68] O. O. Olateju, S. U. Okon, U. T. I. Igwenagu, A. A. Salami, T. O. Oladoyinbo, and O. O. Olaniyi, “Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud,” *Asian Journal of Research in Computer Science*, vol. 17, no. 6, pp. 264–292, Jun. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i6472.
[69] M. Hartmann, U. S. Hashmi, and A. Imran, “Edge computing in smart health care systems: Review, challenges, and research directions,” *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, Aug. 2019, doi: https://doi.org/10.1002/ett.3710.
[70] O. O. Olateju, S. U. Okon, O. O. Olaniyi, A. D. Samuel-Okon, and C. U. Asonze, “Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data,” *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 244–268, Jun. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71206.
[71] A. U. Mahin, S. N. Islam, F. Ahmed, and Md. F. Hossain, “Measurement and monitoring of overhead transmission line sag in smart grid: A review,” *IET Generation, Transmission & Distribution*, vol. 16, no. 1, Aug. 2021, doi: https://doi.org/10.1049/gtd2.12271.
[72] A. A. Salami, U. T. I. Igwenagu, C. E. Mesode, O. O. Olaniyi, and O. B. Oladoyinbo, “Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security,” *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 304–323, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51156.
[73] X. Zhao, Y. Fang, H. Min, X. Wu, W. Wang, and R. Teixeira, “Potential sources of sensor data anomalies for autonomous vehicles: An overview from road vehicle safety perspective,” *Expert Systems with Applications*, vol. 236, p. 121358, Feb. 2024, doi: https://doi.org/10.1016/j.eswa.2023.121358.
[74] V. Chang *et al.*, “A Survey on Intrusion Detection Systems for Fog and Cloud Computing,” *Future Internet*, vol. 14, no. 3, p. 89, Mar. 2022, doi: https://doi.org/10.3390/fi14030089.
[75] A. D. Samuel-Okon, O. I. Akinola, O. O. Olaniyi, O. O. Olateju, and S. A. Ajayi, “Assessing the Effectiveness of Network Security Tools in Mitigating the Impact of Deepfakes AI on Public Trust in Media,” *Archives of Current Research International*, vol. 24, no. 6, pp. 355–375, Jul. 2024, doi: https://doi.org/10.9734/acri/2024/v24i6794.

UNDER PEER REVIEW

[76] T. Theodoropoulos *et al.*, “Security in Cloud-Native Services: A Survey,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 758–793, Dec. 2023, doi: https://doi.org/10.3390/jcp3040034.
[77] S. Daousis, N. Peladarinos, V. Cheimaras, P. Papageorgas, D. D. Piromalis, and R. A. Munteanu, “Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures,” *Future Internet*, vol. 16, no. 1, pp. 33–33, Jan. 2024, doi: https://doi.org/10.3390/fi16010033.
[78] A. D. Samuel-Okon, O. O. Olateju, S. U. Okon, O. O. Olaniyi, and U. T. I. Igwenagu, “Formulating Global Policies and Strategies for Combating Criminal Use and Abuse of Artificial Intelligence,” *Archives of current research international*, vol. 24, no. 5, pp. 612–629, Jun. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5735.
[79] T. Suleski, M. Ahmed, W. Yang, and E. Wang, “A Review of multi-factor Authentication in the Internet of Healthcare Things,” *Digital Health*, vol. 9, no. 1, p. 205520762311771-205520762311771, Jan. 2023, doi: https://doi.org/10.1177/20552076231177144.
[80] J. C. Ugonnia, O. O. Olaniyi, F. G. Olaniyi, A. A. Arigbabu, and T. O. Oladoyinbo, “Towards Sustainable IT Infrastructure: Integrating Green Computing with Data Warehouse and Big Data Technologies to Enhance Efficiency and Environmental Responsibility,” *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 247–261, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51151.
[81] I. H. Sarker, “Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects,” *Annals of Data Science*, vol. 10, pp. 1473–1498, Sep. 2022, doi: https://doi.org/10.1007/s40745-022-00444-2.
[82] B. Kaplan, “PHI Protection under HIPAA: An Overall Analysis,” *papers.ssrn.com*, Oct. 26, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3833983 (accessed Oct. 12, 2024).
[83] D. Sargiotis, “Data Security and Privacy: Protecting Sensitive Information,” *Springer Link*, pp. 217–245, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-67268-2_6.

UNDER PEER REVIEW