Advances in Applied Accounting Research, 3(1), 2025. 41 - 54
DOI: https://doi.org/10.60079/aaar.v3i1.453

OPEN ACCESS
ISSN Online: 2985-8186

Advances in Applied Accounting Research
https://advancesinresearch.id/index.php/AAAR

Digital Government Implementation and its Implications for Accounting Systems and Data Security

Noordiyati ✉ *Fakhri* [2]

✉ *STIE Pancasetia Banjarmasin, Kalimantan Selatan, 70248, Indonesia*
[2] *STIE Pancasetia Banjarmasin, Kalimantan Selatan, 70248, Indonesia*

Received: 2025, 01, 18 **Accepted:** 2025, 01, 30
Available online: 2025, 01, 31

Corresponding author. Noordiyati
✉ *noordiyatitamjiddin@gmail.com*

KEYWORDS

Keywords:
Digital government; public sector accounting; data security; blockchain; transparency.

Conflict of Interest Statement:
The author(s) declare that the research was conducted without any commercial or financial relationships that could be construed as a potential conflict of interest.

ABSTRACT

Purpose: This study investigates the implications of digital government implementation on public sector accounting systems and data security. The purpose is to explore how digital technologies enhance financial management transparency and accountability while addressing the challenges related to data security in public administration.

Research Design and Methodology: This research adopts a qualitative approach, utilizing a systematic literature review (SLR) to analyze relevant studies on digital government, accounting systems, and data security. The methodology involved reviewing recent articles and studies to gain a comprehensive understanding of the subject.

Findings and Discussion: The findings reveal that technologies such as cloud computing, artificial intelligence (AI), machine learning, and blockchain have significantly enhanced the efficiency and accuracy of public sector financial reporting. Blockchain enhances transparency by ensuring the immutability of financial transactions. However, the study also highlights challenges, including cybersecurity risks, data breaches, and the need for comprehensive data governance frameworks. The findings emphasize the importance of human resource preparedness and infrastructure readiness in implementing digital accounting systems effectively.

Implications: The study's practical implications suggest that policymakers must invest in secure digital infrastructure, provide continuous training for government employees, and establish strong data governance frameworks. These strategies are crucial for ensuring the effectiveness, security, and accountability of digital government systems.

Introduction

The unprecedented advancement of digital technologies has reshaped governance in the public sector, giving rise to what is commonly referred to as digital government. This concept represents a shift towards adopting technology-driven processes to enhance transparency, operational efficiency, and the accessibility of public services. Digital government initiatives promote greater citizen engagement, streamline bureaucratic processes, and facilitate data-driven policy decisions. Over the years, these initiatives have evolved to incorporate more advanced tools, such as artificial intelligence (AI), machine learning (ML), and blockchain, to handle increasingly complex administrative tasks and

improve public service delivery (Carayannis et al., 2024). However, significant challenges have emerged alongside these technological advancements, particularly concerning the security, accuracy, and reliability of public financial data. Digital platforms, while improving administrative capabilities, introduce new vulnerabilities in potential data breaches, cyberattacks, and unauthorized access (Srinivas & Liang, 2022). These security threats pose significant concerns regarding the integrity of financial reporting systems, particularly in environments where cybersecurity frameworks are underdeveloped. The global trend toward digital transformation underscores the need for robust governance mechanisms to address these vulnerabilities. Inadequate protection can erode public trust and lead to governance failures, as data integrity and accountability are paramount to effective public sector administration (Gupta et al., 2024). These concerns underscore the complexities of digital government implementation and emphasize the need for a more in-depth examination of the interconnected dynamics between technological advancements and security measures.

In public sector accounting, digital government requires a comprehensive shift in managing, recording, and reporting financial data (Alsharari & Ikem, 2023). Automated and real-time accounting systems, integrated within digital frameworks, offer significant advantages, including enhanced accuracy, operational efficiency, and streamlined reporting processes (Sonjaya, 2024). These systems can minimize human error, accelerate the preparation of financial reports, and facilitate oversight through more transparent data flows. Despite these benefits, the transition to digital systems brings heightened security challenges, necessitating robust cybersecurity protocols to safeguard data from potential disruptions. A central issue is the extent to which public institutions are prepared to maintain the reliability and integrity of financial reporting in the face of escalating cyber threats. This issue is particularly pressing in developing nations, where budget constraints, limited technical capacity, and institutional resistance to change impede the seamless adoption of secure digital solutions. The rise in cyber incidents targeting public financial systems has intensified scrutiny of digital government initiatives, raising questions about the readiness of governments to deploy comprehensive and secure digital accounting frameworks (Uddin et al., 2020). When poorly managed or inadequately protected, digital financial systems risk compromising public accountability and undermining governance structures, potentially leading to public distrust in government institutions (Grossi & Argento, 2022). This study, therefore, examines the broader implications of digital government implementation for public sector accounting systems, with a specific focus on data security as a crucial element in ensuring sustainable governance and public accountability.

Recent studies have highlighted the significant role of digital technologies in improving public sector accounting processes. Novichenko et al. (2024) emphasized that digital accounting systems (DAS) enhance efficiency, accuracy, and analytical capabilities through automation, real-time data processing, and advanced analytics. These systems contribute to transparency and accountability in financial reporting, which is crucial for fraud prevention and fostering good governance (Panggeso et al., 2024). However, challenges such as data security issues, the need for specialized training, and high implementation costs remain significant obstacles (Ibrahim & Tahir, 2024). Furthermore, the evolving role of accountants in the digital age necessitates new competencies in information technology, robotic process automation (RPA), and artificial intelligence (AI) to adapt effectively to these advancements (Ibrahim & Tahir, 2024). Duan et al. (2023) further noted that social media data could improve accountability and decision-making in public sector accounting, indicating a trend toward more integrated and data-driven governance. Research on integrating AI, machine learning (ML), and blockchain has shown potential for real-time processing and enhanced fraud detection. However, data security remains a concern, particularly in the absence of robust cybersecurity frameworks (Novichenko et al., 2024). Alsharari & Ikem (2023) explored the reciprocal relationship between digital accounting systems and organizational processes, highlighting procedural changes. However, digital public services also raise accountability challenges, such as blurred roles and the need for inclusive governance (Agostino et al., 2022). These findings underscore that digital government initiatives can improve efficiency but also pose complexities that warrant further exploration.

Despite extensive research on digital government and public sector accounting, significant gaps persist in the literature. While studies by Novichenko et al. (2024), Panggeso et al. (2024), and Ibrahim

& Tahir (2024) highlight the advantages and challenges of digital accounting systems (DAS), such as increased efficiency and the need for specialized training, few studies provide a comprehensive examination of how digital government initiatives impact public financial data security. Existing research often isolates specific aspects, such as automation and real-time processing, without fully addressing how these technological advancements influence data integrity and public trust. Although Alsharari & Ikem (2023) explored organizational and procedural changes driven by digital systems, and Agostino et al. (2021) discussed accountability issues, their findings do not adequately account for the technical and cultural barriers that hinder secure and effective implementation. There is limited exploration of the intersection between advanced technologies, such as artificial intelligence (AI) and blockchain, and cybersecurity risks within the public sector. While some studies acknowledge the vulnerabilities introduced by these innovations, the question of how governments can strike a balance between adopting technological advancements and maintaining robust data security remains largely unanswered. This gap highlights the need for a comprehensive analysis that considers the technical efficiencies provided by digital government systems and the governance frameworks necessary to safeguard public financial data and ensure accountability during digital transformation.

This study addresses the identified research gaps by conducting a systematic literature review (SLR) to explore the implications of digital government implementation for accounting systems and data security. The novelty of this research lies in its holistic approach, which examines not only technical aspects—such as automation, real-time data processing, and fraud detection—but also governance dimensions, including transparency, accountability, and data protection measures. Unlike previous studies that tend to focus on isolated elements, this research integrates multiple perspectives to identify best practices and potential risks associated with digital financial management in the public sector. By synthesizing findings from various studies, this research aims to elucidate the relationship between technological advancements and efforts to preserve the integrity of public financial data. The primary research question guiding this study is: How does implementing digital government initiatives affect the accuracy, efficiency, and security of public sector accounting systems? This research addresses the question: What measures can be implemented to mitigate data security risks within digital public sector accounting frameworks? The study has two main objectives: (1) to analyze the benefits and limitations of digital accounting systems within digital government frameworks and (2) to identify the key challenges and vulnerabilities related to data security in public financial reporting. By bridging existing research gaps, this study is expected to contribute to the development of more accountable and resilient public sector accounting systems in the digital era of transformation.

Literature Review

Agency Theory as a Framework for Understanding Accountability in Digital Government

In the context of digital government, the principal-agent relationship refers to the interaction between citizens, who are principals with the right to access public services, and public officials, who are agents tasked with managing public resources under a specific mandate (Gauld, 2018). However, this relationship is prone to information asymmetry, where agents have exclusive access to financial information that is not publicly available. Digital accounting systems (DAS) aim to reduce this asymmetry by providing real-time, accessible, and verifiable financial data (Mikhalkina et al., 2020). These systems enhance transparency and foster public trust in government financial management by offering real-time reporting. Several countries have successfully implemented digital reporting platforms that strengthen public oversight through open access to financial records (Ivaninskiy et al., 2023). However, accountability challenges persist when public officials' incentives do not align with public service goals, which can lead to opportunistic behavior. In some cases, automation, such as machine learning and artificial intelligence (AI), shifts accountability from human officials to algorithms, complicating public understanding of financial processes (Sukhwal & Kankanhalli, 2022). The complexity of such systems can create new layers of opacity, undermining transparency efforts. Additionally, automated decision-making can reduce human oversight, leaving room for systemic errors that compromise the accuracy of reporting (Gong et al., 2025). These issues underscore the importance of robust data governance in ensuring that digital financial systems enhance reporting efficiency and maintain public accountability. Therefore, while DAS offers significant benefits, it

necessitates a comprehensive governance framework to mitigate potential risks and maintain public trust in financial management.

Technology significantly addresses agency problems by enhancing transparency and accountability through immutable and traceable data (Secinaro et al., 2022). Blockchain, for instance, has been recognized for its ability to permanently record financial transactions, making them accessible for automated audits and public verification. According to Tyma et al. (2022), blockchain-based systems introduce novel accountability mechanisms that distribute oversight responsibilities across participants, fostering a more transparent financial reporting environment. These systems narrow the information gap between public officials and citizens by enabling real-time access to data, thereby facilitating public oversight and enhancing fiscal decision-making (Roggenkamp, 2023). However, successfully implementing such technologies depends on adequate infrastructure and comprehensive training for human resources. Secinaro et al. (2022) emphasize that integrating blockchain into public-sector accounting necessitates substantial investments, particularly in developing countries, where resource constraints can impede digital adoption. Data privacy and security concerns remain critical, especially when large volumes of sensitive data are processed. The potential for data breaches can undermine public trust in digital systems despite their benefits in creating transparency. Gadallah (2023) emphasizes that the role of blockchain in addressing development challenges depends on its alignment with robust governance frameworks that regulate data usage and ensure public accountability. Therefore, while blockchain-based reporting systems offer promising solutions for agency problems, their effectiveness relies on strong governance, continuous monitoring, and investments in cybersecurity to prevent unintended consequences of automation and maintain public trust in digital financial management.

Digital Government

Digital government refers to the adoption of digital technologies to enhance public service delivery, improve administrative processes, and promote transparency and accountability. This transformation leverages cloud computing, artificial intelligence (AI), machine learning (ML), and blockchain to facilitate efficient data management and informed decision-making (Wirtz, 2022). The successful implementation of digital government services requires more than just technological infrastructure; it necessitates institutional readiness, effective regulatory frameworks, and active citizen engagement (Kumar, 2024). While digital platforms enable the secure storage of large datasets and real-time reporting, they also underscore the importance of interoperability and user-centric design to ensure public accessibility (Huang et al., 2019). However, implementing digital government initiatives faces significant challenges, particularly in developing countries where connectivity and resources are limited. Cordella & Paletti (2019) point out that fragmented infrastructures can hinder the orchestration of digital services, limiting the government's ability to deliver integrated solutions. A lack of digital literacy among public officials can slow the adoption process, as inadequate training leads to errors in data management and system use. Moreover, institutional resistance to adopting new technologies often stems from concerns about transparency, control, and accountability (Meijer & Bolívar, 2016). To overcome these barriers, robust governance frameworks must protect data privacy while fostering transparency. This dual focus can increase public trust in digital governance and strengthen the role of technology as a driver of bureaucratic reform, enabling more efficient and equitable access to government services and data.

Implementing digital government initiatives presents numerous challenges despite their potential benefits in improving public services and transparency. A significant barrier is the lack of adequate digital infrastructure, including inconsistent internet connectivity and outdated hardware. The digital transformation process is significantly hindered without robust infrastructure, especially in remote regions (Antipina et al., 2022). The disparity in technological access exacerbates the digital divide between urban and rural areas, making it challenging to achieve equitable public service delivery. Additionally, low digital literacy among public officials remains a critical issue. Samsor (2021) highlights that inadequate training and limited technical expertise among government employees slow the adoption of new systems and increase the likelihood of errors in financial data management. Institutional resistance to change also plays a significant role in delaying the implementation of digital

systems. This resistance is often linked to fears of diminished control and perception, as well as the complexity of new procedures (Oseni, 2024). Therefore, a robust governance framework that includes clear data privacy and security policies is crucial for fostering trust and compliance. Such governance structures can help mitigate the misuse of digital technologies in managing sensitive government data, such as financial reports. Case studies in nations with established data governance policies demonstrate that stringent data protection measures can enhance public trust in digital platforms, thereby reinforcing their legitimacy and effectiveness (Çubuk et al., 2021). By addressing these challenges, digital government can be a powerful tool for bureaucratic reform and increase public trust.

Public Sector Accounting Systems in the Digital Era

The transformation of public sector accounting systems from manual, paper-based processes to digital and automated frameworks has significantly improved financial management and reporting accuracy. Digital Accounting Systems (DAS) play a pivotal role in enabling real-time financial reporting, minimizing human errors, and enhancing oversight of government expenditures (Prasetianingrum & Sonjaya, 2024). Yang (2024) highlights that cloud-based systems and machine learning enable more sophisticated data analysis, supporting evidence-based policy decisions. Moreover, the integration of artificial intelligence (AI) facilitates the identification of financial discrepancies and automates routine accounting tasks, thereby improving overall efficiency (Secinaro et al., 2022). In countries such as Estonia and Singapore, DAS implementations have demonstrated the potential to streamline reporting processes and improve transparency by providing stakeholders with timely access to financial data. However, effective implementation also requires robust infrastructure and skilled personnel. According to Alsharari & Ikem (2023), the mutual interaction between digital tools and organizational workflows necessitates procedural adjustments and the redefinition of staff roles to avoid operational bottlenecks. Without these changes, the benefits of DAS may be undermined by inefficiencies and errors. Broccardo et al. (2023) also emphasize the need for robust governance frameworks to safeguard data integrity and prevent misuse, ensuring public trust in financial reporting. By addressing these technological and organizational factors, DAS can reinforce public accountability and enhance the credibility of government financial management.

The successful implementation of Digital Accounting Systems (DAS) in the public sector relies not only on advanced technology but also on the readiness of human resources to operate these systems effectively. Technologies such as robotic process automation (RPA), artificial intelligence (AI), and blockchain require public sector accountants to develop new technical competencies (Schlegel & Kraus, 2023). Without appropriate training, employees may struggle to adapt to these innovations, increasing the risk of operational errors in financial reporting. Digital transformation must be accompanied by comprehensive training programs that strengthen the digital literacy of government employees, ensuring smooth transitions to automated processes (Shibambu & Ngoepe, 2024). In addition to capacity-building efforts, robust IT infrastructure is essential for DAS to function reliably. Fikri et al. (2019) emphasize that stable internet connectivity and compatible hardware are necessary for supporting real-time financial reporting and data integration. However, even with advanced infrastructure, governance frameworks play a pivotal role in regulating system operations. Alsharari & Ikem (2023) argue that clear policies related to data security and operational standards are necessary to maintain the integrity of financial data and prevent unauthorized access. Countries with established regulatory frameworks have demonstrated that transparent and secure DAS implementations can foster public trust and enhance accountability. Therefore, developing an effective public sector accounting system requires a synergistic approach that integrates technological advancements, human resource development, and sound policy frameworks to support sustainable financial governance.

Data Security in Digital Government Systems

Data security is a critical component of digital government systems, particularly in financial reporting, as it safeguards public trust by ensuring confidentiality, integrity, and availability of financial data (Haapamäki & Sihvonen, 2019). Sharma (2020) emphasizes that a breach of these principles can severely undermine public confidence and government legitimacy, as incidents of

financial data leaks often lead to public outrage and distrust. In the face of increasing cyberattacks such as hacking, ransomware, and data breaches, Ramos & Ellul (2024) highlight the importance of robust cybersecurity governance. They argue that adopting new technologies, such as AI and blockchain, without an adequate security framework introduces vulnerabilities that cybercriminals can exploit. While AI enhances fraud detection and automates security processes, it also presents challenges related to transparency and accountability in public sector financial management (Ahmad et al., 2025). This highlights the importance of striking a balance between the adoption of technology and regulatory oversight. Effective security strategies, including encryption, firewalls, and multi-factor authentication, are crucial for preventing unauthorized access and safeguarding sensitive financial data. Barezzani (2019) emphasizes the significance of international regulatory frameworks, such as the General Data Protection Regulation (GDPR), which has established a global standard for data privacy and security governance. Similar regulatory measures can enhance data protection in digital financial reporting systems, ensuring public trust and resilience against cyber threats. Thus, data security must remain a top priority in digital government systems to support transparency, accountability, and secure service delivery.

Strengthening data security in digital government systems requires a comprehensive approach integrating technological measures, governance frameworks, and strategic collaborations. Matheus et al. (2020) argue that data security in the public sector is not just a technical issue but also a governance challenge that demands a holistic strategy involving clear regulations and robust oversight mechanisms. Encryption is one of the most effective methods for protecting sensitive financial data, ensuring that information remains unreadable to unauthorized users. Integrating encryption with multi-factor authentication (MFA) significantly enhances system security by adding multiple layers of verification, making unauthorized access increasingly difficult (Ogbanufe & Baham, 2023). However, simply implementing these technologies is not enough. Bouke (2023) highlights the importance of regular system audits to identify vulnerabilities and address security gaps before cyberattacks occur. Such proactive measures can mitigate the risks associated with data breaches and ransomware attacks, which have become increasingly sophisticated. Collaboration with technology experts and private organizations is crucial to ensure that data security policies remain adaptable to evolving threats. Moreover, adopting international regulatory frameworks, such as the General Data Protection Regulation (GDPR), has proven effective in reinforcing public sector accountability. Mesarčík & Hamuľák (2024) note that GDPR's stringent data privacy provisions have set a global benchmark for data governance, emphasizing the need for government accountability in handling sensitive information. These combined efforts can enhance public trust and improve the resilience of financial reporting systems against cyber threats, ensuring transparent and secure digital government operations.

Research Design and Methodology

Study Design

This research employs a qualitative approach using the Systematic Literature Review (SLR) method. The SLR method is chosen to synthesize and critically evaluate relevant academic literature on data security in digital government systems. Following established guidelines, the study employs a structured process that involves identifying, selecting, and analyzing peer-reviewed articles to ensure reliability and validity. By systematically reviewing existing research, this study aims to gain a comprehensive understanding of key themes, challenges, and best practices in securing digital financial reporting systems.

Sample Population or Subject of Research

The subject of this research comprises academic journals, conference proceedings, and books from reputable databases, including Elsevier, Emerald, Wiley, and Springer. The inclusion criteria focus on articles published after 2015 to ensure the review remains current and relevant to contemporary developments. The sample includes studies that address data security frameworks, digital government implementation, and regulatory impacts, particularly those related to financial reporting in the public sector.

Data Collection Techniques and Instrument Development

Data collection is conducted by systematically searching databases using predefined keywords such as "digital government," "data security," "financial reporting," and "cybersecurity governance." The search strategy incorporates Boolean operators to refine the results and exclude irrelevant publications. A coding framework is developed to categorize findings based on key themes, including data protection strategies, governance policies, and cybersecurity challenges.

Data Analysis Techniques

The collected data are analyzed using thematic analysis to identify recurring patterns and draw meaningful conclusions. Each article is reviewed for its contributions to the research questions, and the findings are synthesized to highlight both consistencies and gaps in the literature. The analysis also involves comparing the effectiveness of regulatory frameworks, such as the General Data Protection Regulation (GDPR), across different contexts to provide practical recommendations for enhancing data security in digital government systems.

Findings and Discussion

Findings

The implementation of digital government in public sector accounting systems has significantly transformed financial management processes, particularly in data recording, reporting, and analysis. The shift from manual to automated systems has improved efficiency, accuracy, and access to real-time financial data. Cloud computing enables centralized and secure data storage, allowing for faster data access and seamless sharing across departments (Alsharari & Ikem, 2023). These systems reduce operational delays and foster cross-agency collaboration in public financial management. Moreover, AI and machine learning enhance decision-making processes by identifying financial patterns and generating predictive analytics that support resource allocation (Carayannis et al., 2024). Blockchain technology, conversely, ensures the immutability of transaction records, strengthening the credibility of public sector financial reports (Gadallah, 2023). Countries such as Estonia and Singapore have demonstrated the success of digital transformations, showcasing how integrated digital systems can enhance governance and foster public trust (Çubuk et al., 2021). However, effective implementation requires more than advanced technology—it also relies on regulatory frameworks, institutional readiness, and organizational leadership (Cordella & Paletti, 2019). The absence of these supporting elements can hinder the adoption of digital accounting systems, underscoring the need for comprehensive strategies that include policy and technological innovation to ensure transparency and accountability in public financial reporting.

Digital technologies are vital in enhancing transparency and accountability in public sector accounting by addressing information asymmetry between government institutions and citizens. Real-time access to financial data empowers citizens to monitor government activities, thus increasing their participation in public financial oversight (Prasetianingrum & Sonjaya, 2024). These technologies foster public trust in governmental processes by ensuring the availability and traceability of financial information. Blockchain technology strengthens public confidence by enabling verifiable and immutable records that prevent unauthorized alterations to financial transactions (Ramos & Ellul, 2024). Such features enhance the legitimacy of public financial reports and reinforce the accountability of public officials. However, while these advancements mitigate some transparency issues, they also present challenges related to data governance and security. Poorly implemented digital systems can create vulnerabilities that malicious actors may exploit, highlighting the importance of robust cybersecurity frameworks (Grossi & Argento, 2022). Furthermore, the success of transparency initiatives relies on clear governance policies that govern the use and protection of public financial data (Çubuk et al., 2021). Digital tools may unintentionally contribute to further information gaps or even data misuse without proper oversight and control. Therefore, strengthening data governance through well-defined policies and active public engagement is essential to ensure technological advancements support transparency goals rather than compromise them.

Despite the numerous advantages of digital government systems, they face significant risks and challenges, particularly in data security. Cyber threats, including hacking, ransomware attacks, and data breaches, pose considerable risks to the integrity of public financial data (Haapamäki & Sihvonen, 2019). Economic data that is inadequately protected can become a prime target for cybercriminals, potentially disrupting public services and losing public trust. Public institutions that lack robust cybersecurity frameworks are particularly vulnerable to these threats (Srinivas & Liang, 2022). In addition to external cyberattacks, internal weaknesses such as outdated security protocols, insufficient staff training, and a lack of crisis response plans exacerbate these vulnerabilities (Ivaninskiy et al., 2023). Digital systems without comprehensive governance policies and security safeguards can be prone to operational errors and data manipulation, further jeopardizing public financial reporting. Moreover, as digital systems become more complex, the risks associated with interoperability and data sharing increase (Çubuk et al., 2021). Addressing these risks requires a multi-pronged approach, including regular system audits, updated cybersecurity measures, and staff training programs focused on data protection. Regulatory frameworks that mandate compliance with international data protection standards, such as GDPR, can also reinforce institutional accountability and resilience in the face of cyber threats (Mesarčík & Hamuľák, 2024). Strengthening security frameworks is critical for ensuring the continuity and credibility of digital financial systems.

Human resource readiness is crucial for the successful implementation of digital accounting systems in the public sector. To fully utilize digital systems, public sector employees must develop competencies in emerging technologies such as robotic process automation (RPA), AI, and blockchain (Schlegel & Kraus, 2023). However, many government institutions face challenges related to inadequate training programs and limited resources for continuous professional development (Ahmad et al., 2025). Employees who lack sufficient digital literacy may struggle to adapt to automated systems, resulting in inefficiencies and errors in financial reporting. Therefore, comprehensive training initiatives are necessary to build technical competencies and ensure smooth transitions to computerized processes (Shibambu & Ngoepe, 2024). Effective training programs should cover technical skills and emphasize the importance of data security and compliance with regulatory standards (Alsharari & Ikem, 2023). Government agencies must allocate resources to create a supportive learning environment that encourages skill enhancement and innovation.

Collaboration with academic institutions and private sector experts can also strengthen workforce capacity and foster knowledge exchange. Building a digitally literate workforce improves institutional resilience and enhances the public sector's ability to manage complex financial systems (Prasetianingrum & Sonjaya, 2024). Ultimately, a well-trained workforce contributes to the overall success of digital governance initiatives by ensuring that new technologies are utilized effectively and responsibly.

Data governance policies are crucial in safeguarding public financial systems and ensuring transparency and accountability. Regulations such as the General Data Protection Regulation (GDPR) have established global benchmarks for data protection and public sector accountability (Barezzani, 2019). GDPR emphasizes the rights of individuals over their data and obliges institutions to implement stringent data protection measures. Countries that have adopted GDPR-inspired frameworks have reported increased public trust and improved transparency in financial reporting (Mesarčík & Hamuľák, 2024). Effective data governance necessitates regulatory compliance and proactive measures, including routine audits, incident response protocols, and stakeholder collaboration, to maintain data integrity and resilience (Bouke, 2023). These policies help mitigate privacy risks and protect sensitive information from unauthorized access (Sharma, 2020).

Additionally, comprehensive data governance frameworks support the integration of digital tools by defining clear responsibilities for data management and security (Cordella & Paletti, 2019). Public institutions that adopt robust governance practices are better equipped to handle data-related challenges and recover from cyber incidents swiftly (Ramos & Ellul, 2024). By reinforcing accountability and ensuring data transparency, effective data governance frameworks enhance the legitimacy of digital government systems and foster public confidence. Strong governance protects institutional data and builds resilience, allowing public sector entities to leverage technological advancements without compromising security.

Discussion

The findings of this study offer an in-depth examination of how digital government initiatives, particularly in the realm of public sector accounting, have transformed the management of public financial data. A significant observation from this research is the pivotal role of emerging digital technologies—such as cloud computing, artificial intelligence (AI), machine learning, and blockchain—in transforming the processes involved in recording, reporting, and managing financial information within the public sector. These technologies have introduced considerable improvements, including enabling real-time financial reporting, enhancing data processing accuracy, and reducing the likelihood of human error. As a result, the public sector is witnessing more efficient and timely financial reporting, which facilitates the creation of a more transparent and accountable system. Stakeholders, including citizens and policymakers, now have access to updated financial data at any time, fostering a greater sense of trust and engagement. A critical technological advancement is blockchain technology, which provides a permanent and immutable record of transactions. This ensures the accuracy and authenticity of public financial data, significantly strengthening public trust in government financial systems. Moreover, integrating AI and machine learning into accounting systems has further enhanced the ability to detect anomalies and fraudulent activities, thereby increasing the overall integrity of public sector financial reports. This finding supports earlier research by Novichenko et al. (2024) and Alsharari and Ikem (2023), highlighting how digital systems reduce information asymmetry and improve accountability in public sector operations.

While the advancements brought about by digital technologies in public-sector accounting have brought about positive changes, the study also identified significant challenges, particularly in data security. Although the integration of digital tools has greatly enhanced transparency, these same technologies have also opened the door to new risks, particularly in protecting sensitive public financial data. Cybersecurity threats, including cyberattacks, data breaches, and unauthorized access to critical economic systems, have become pressing concerns, particularly in countries where cybersecurity infrastructure remains underdeveloped. This highlights the importance of implementing robust data governance frameworks to safeguard sensitive information and protect the integrity of financial data. In countries where cybersecurity measures are not sufficiently developed, the risks to public financial data are particularly acute. As Ibrahim and Tahir (2024) pointed out, digital government systems risk inadvertently exposing public financial data to cyber threats without proper security protocols, which could undermine the transparency and accountability they aim to promote. This finding highlights the urgent need for governments to prioritize cybersecurity and invest in enhancing their digital defense systems. It also underscores the need for a strategic approach to digital governance that includes not only technological investments but also robust policies and frameworks to protect the integrity of public data. Given the increasing prevalence of cyber incidents worldwide, governments must develop strong and secure digital systems to maintain trust and encourage continued participation among citizens.

The research findings also highlight the crucial role that human resource preparedness plays in the effective implementation of digital accounting systems within the public sector. While digital technologies offer significant advantages in terms of efficiency and transparency, the study reveals that the success of these systems may be compromised without adequate human resource development. Public sector accountants, in particular, need to develop competencies in emerging technologies such as robotic process automation (RPA), AI, and blockchain. The ability to effectively operate these technologies is crucial to fully realizing the potential of digital accounting systems. However, the study found that many public sector employees lack sufficient training to effectively navigate these advanced systems, which could lead to operational errors and inaccuracies in financial reporting. This finding highlights the importance of ongoing training and professional development programs in enhancing the digital literacy of government employees. As public sector accounting becomes increasingly reliant on digital tools, training in AI, machine learning, and blockchain technologies will become crucial to ensure that staff can operate the systems effectively and accurately. The research also highlighted the importance of having a robust infrastructure to support the effective operation of these systems. Adopting real-time financial reporting systems remains a

significant challenge in many developing countries, where internet connectivity is unreliable and hardware is outdated. Without the proper technological infrastructure, even the most sophisticated digital accounting systems cannot operate at their full potential. Therefore, governments must address these infrastructure gaps and invest in the development of technological and human resources to ensure that digital accounting systems are implemented and maintained effectively.

From a theoretical standpoint, the study's findings closely align with principal-agent theory, providing valuable insights into the dynamics of digital governance. The principal-agent theory focuses on the relationship between citizens, who are the principals with the right to public services, and public officials, who are the agents responsible for managing public resources on behalf of the citizens. In digital accounting systems, the relationship between principals and agents is increasingly mediated by technological advancements that facilitate transparency and accountability. Adopting digital systems, such as blockchain, addresses the principal-agent problem by reducing information asymmetry between citizens and public officials. Blockchain enables the real-time verification of public financial transactions, providing citizens with direct access to information and thereby enhancing trust in the system. This aligns with the premise that transparency is a key mechanism for mitigating the potential conflicts inherent in the principal-agent relationship, where agents may otherwise act in ways that benefit themselves rather than the public. The findings also support the idea that technology can help reduce agency costs by holding public officials accountable for their actions. As Alsharari and Ikem (2023) noted, integrating digital technologies in public sector accounting enhances the interplay between technology and governance frameworks, leading to more efficient and accountable administrative processes. By leveraging transparent digital systems, governments can foster a more effective and trustworthy relationship with their citizens, ensuring that public officials act in the best interests of the people they serve.

Compared to previous studies, the findings of this research align with much of the existing literature on digital government and public sector accounting, reaffirming the positive effects of technological advancements in enhancing transparency and accountability. Studies such as those by Novichenko et al. (2024) and Alsharari and Ikem (2023) have highlighted the role of digital accounting systems in enhancing accuracy in financial reporting by reducing human errors and streamlining processes. These findings are consistent with the results of this study, which highlight the crucial role that technologies such as blockchain, artificial intelligence (AI), and machine learning play in enhancing the efficiency and accuracy of public financial management. However, this research goes beyond previous studies by addressing the increasing concerns surrounding data security and the need for robust data governance frameworks. While earlier studies recognized the importance of cybersecurity, this research takes a deeper dive into the risks posed by cyberattacks, data breaches, and unauthorized access to public financial data, stressing the urgency of implementing comprehensive cybersecurity measures. Another area where this research contributes to the literature is its focus on human resource challenges, a topic often overlooked in previous studies. While many studies focus on technological infrastructure, this study emphasizes the importance of providing adequate training and development programs for public sector employees. This perspective aligns with the findings of Agostino et al. (2022), who emphasize the importance of human capital in ensuring the success of digital transformation in public services. Without proper human resource preparedness, the full potential of digital accounting systems cannot be effectively harnessed, making it a crucial factor for successful implementation.

The practical implications of these findings are of paramount importance for policymakers and public administrators, providing a roadmap for enhancing the effectiveness and security of digital government systems. First and foremost, the research underscores the crucial need for governments to invest in robust digital infrastructure and effective cybersecurity measures to safeguard public financial data. Governments should prioritize the development of secure, reliable, and scalable digital systems that are resilient to emerging cyber threats. These systems must be equipped with advanced security features, such as encryption, multi-factor authentication, and real-time monitoring, to ensure the integrity and confidentiality of financial data. Second, the findings highlight the need for ongoing training programs to enhance the digital literacy of public sector employees. Governments must provide comprehensive training that equips employees with the skills to effectively utilize emerging

technologies such as artificial intelligence, machine learning, and blockchain. These training initiatives should not only focus on the operational aspects of these technologies but also address cybersecurity risks and protocols, ensuring that employees can recognize and mitigate potential security threats. Ultimately, the research highlights the importance of establishing robust data governance frameworks to safeguard public financial data. Governments should implement clear, transparent policies and regulations that protect the privacy and security of sensitive information. Drawing on successful models like the General Data Protection Regulation (GDPR), governments can develop comprehensive data protection frameworks that foster public trust and enhance the accountability of digital accounting systems. By incorporating these strategies, governments can ensure that their digital accounting systems are secure, transparent, and accountable to the public.

Conclusion

This study explored the implications of digital government implementation on public sector accounting systems and data security. The findings indicate that integrating technologies such as cloud computing, artificial intelligence (AI), machine learning, and blockchain have significantly transformed financial data management in the public sector. These technologies have enhanced the transparency, accuracy, and efficiency of financial reporting, reduced human error, and ensured real-time access to financial data. Blockchain has emerged as a powerful tool for guaranteeing the authenticity and traceability of financial transactions. However, the study also uncovered several challenges, particularly about cybersecurity risks, data breaches, and the need for robust data governance frameworks. It highlighted that the benefits of digital systems could be undermined without adequate resources, cybersecurity measures, and employee training.

The value of this study lies in its contribution to both the academic understanding and practical application of digital government. It offers new insights into how, when implemented effectively, digital technologies can transform public financial management, improve accountability, and enhance the trust between governments and citizens. Additionally, the study emphasizes the importance of developing comprehensive data governance frameworks and investing in human capital to ensure the successful implementation of digital systems. For practitioners and policymakers, the study offers actionable recommendations to establish resilient and secure digital government frameworks, ensuring that these technologies enhance transparency and accountability in public administration.

Despite its contributions, the study has certain limitations. One of the key limitations is the focus on the experiences of a few countries, which may not fully represent the global landscape of digital government implementation. Future research could expand the scope of the study to include a broader range of countries, particularly those in developing regions, to gain a deeper understanding of the unique challenges they face. Furthermore, further investigation into the long-term impacts of digital government on public trust and governance structures is needed. Researchers could explore how digital systems evolve and how public sector institutions adapt to technological advancements. The findings of this study provide a foundation for future research on the intersection of technology, governance, and public accountability, urging scholars to explore these dynamics in greater detail.

References

Agostino, D., Saliterer, I., & Steccolini, I. (2022). Digitalization, accounting and accountability: A literature review and reflections on future research in public services. *Financial Accountability & Management*, *38*(2), 152–176. https://doi.org/10.1111/faam.12301

Ahmad, W., Vashist, A., Sinha, N., Prasad, M., Shrivastava, V., & Muzamal, J. H. (2025). *Enhancing Transparency and Privacy in Financial Fraud Detection: The Integration of Explainable AI and Federated Learning BT - Software and Data Engineering* (W. Feng, N. Rahimi, & V. Margapuri (eds.); pp. 139–156). Springer Nature Switzerland.

Alsharari, N. M., & Ikem, F. (2023). Digital accounting systems and information technology in the public sector: mutual interaction. *Journal of Systems and Information Technology*, *25*(1), 53–73. https://doi.org/10.1108/JSIT-09-2021-0190

Antipina, O., Kireeva, E., Ilyashevich, N., & Odoeva, O. (2022). *Digitalization of Regional Economies in the Context of Innovative Development of the Country BT - Digital and Information Technologies in Economics and Management* (A. Gibadullin (ed.); pp. 224–235). Springer International Publishing.

Barezzani, S. (2019). *General Data Protection Regulation (GDPR) BT - Encyclopedia of Cryptography, Security and Privacy* (S. Jajodia, P. Samarati, & M. Yung (eds.); pp. 1–6). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-27739-9_1811-1

Bouke, M. A. (2023). *Security Assessment and Testing BT - CISSP Exam Certification Companion: 1000+ Practice Questions and Expert Strategies for Passing the CISSP Exam* (M. A. Bouke (ed.); pp. 485–567). Apress. https://doi.org/10.1007/979-8-8688-0057-3_8

Broccardo, L., Truant, E., & Argento, D. (2023). *Digitalization and Management Control in the Public Sector: What is Next? BT - Handbook of Big Data and Analytics in Accounting and Auditing* (T. Rana, J. Svanberg, P. Öhman, & A. Lowe (eds.); pp. 279–308). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-4460-4_13

Carayannis, E. G., Askounis, D., Andoutropoulou, M., & Zotas, N. (2024). Leveraging AI for Enhanced eGovernment: Optimizing the Use of Open Governmental Data. *Journal of the Knowledge Economy*. https://doi.org/10.1007/s13132-024-02317-w

Cordella, A., & Paletti, A. (2019). Government as a platform, orchestration, and public value creation: The Italian case. *Government Information Quarterly*, *36*(4), 101409. https://doi.org/https://doi.org/10.1016/j.giq.2019.101409

Çubuk, E. B. S., Demirdöven, B., & Janssen, M. (2021). *Policies for Enhancing Public Trust and Avoiding Distrust in Digital Government During Pandemics: Insights from a Systematic Literature Review BT - Pandemic, Lockdown, and Digital Transformation: Challenges and Opportunities for Public Administration, NGOs, and Businesses* (S. Saeed, M. P. Rodríguez Bolívar, & R. Thurasamy (eds.); pp. 1–23). Springer International Publishing. https://doi.org/10.1007/978-3-030-86274-9_1

Duan, H. K., Vasarhelyi, M. A., Codesso, M., & Alzamil, Z. (2023). Enhancing the government accounting information systems using social media information: An application of text mining and machine learning. *International Journal of Accounting Information Systems*, *48*, 100600. https://doi.org/https://doi.org/10.1016/j.accinf.2022.100600

Fikri, N., Rida, M., Abghour, N., Moussaid, K., & El Omri, A. (2019). An adaptive and real-time based architecture for financial data integration. *Journal of Big Data*, *6*(1), 97. https://doi.org/10.1186/s40537-019-0260-x

Gadallah, K. (2023). *The Potential Role of Blockchain Technology in Addressing Development Challenges in Developing Countries BT - Cutting-Edge Business Technologies in the Big Data Era* (S. G. Yaseen (ed.); pp. 226–236). Springer Nature Switzerland.

Gauld, R. (2018). *Principal-Agent Theory of Organizations BT - Global Encyclopedia of Public Administration, Public Policy, and Governance* (A. Farazmand (ed.); pp. 4914–4918). Springer International Publishing. https://doi.org/10.1007/978-3-319-20928-9_72

Gong, Q., Gai, L., Wang, Y., Xu, D., & Yang, R. (2025). *Approximating Principal-Agent Problem Under Bayesian BT - Frontiers of Algorithmics* (B. Li, M. Li, & X. Sun (eds.); pp. 185–198). Springer Nature Singapore.

Grossi, G., & Argento, D. (2022). The fate of accounting for public governance development. *Accounting, Auditing & Accountability Journal*, *35*(9), 272–303. https://doi.org/10.1108/AAAJ-11-2020-5001

Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J. J. M., & Dwivedi, Y. K. (2024). Trust, Risk, Privacy and Security in e-Government Use: Insights from a MASEM Analysis. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-024-10497-8

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Huang, R., Wang, C., Zhang, X., Wu, D., & Xie, Q. (2019). Design, develop and evaluate an open government data platform: a user-centred approach. *The Electronic Library*, *37*(3), 550–562. https://doi.org/10.1108/EL-02-2019-0037

Ibrahim, A. G., & Tahir, K. M. (2024). The impact of digital accounting technologies in achieving the quality of accounting InformationAmmar. *2024 V International Conference on Neural Networks and Neurotechnologies (NeuroNT)*, 53–57. https://doi.org/10.1109/NeuroNT62606.2024.10585430

Ivaninskiy, I., Ivashkovskaya, I., & McCahery, J. A. (2023). Does digitalization mitigate or intensify the principal-agent conflict in a firm? *Journal of Management and Governance*, *27*(3), 695–725. https://doi.org/10.1007/s10997-021-09584-8

Kumar, D. P. (2024). *The Impact of Digital Technologies on E-Governance: A Comprehensive Analysis BT - Transfer, Diffusion and Adoption of Next-Generation Digital Technologies* (S. K. Sharma, Y. K. Dwivedi, B. Metri, B. Lal, & A. Elbanna (eds.); pp. 367–378). Springer Nature Switzerland.

Matheus, R., Janssen, M., & Maheshwari, D. (2020). Data science empowering the public: Data-driven dashboards for transparent and accountable decision-making in smart cities. *Government Information Quarterly*, *37*(3), 101284. https://doi.org/https://doi.org/10.1016/j.giq.2018.01.006

Meijer, A., & Bolívar, M. P. R. (2016). Governing the smart city: a review of the literature on smart urban governance. *International Review of Administrative Sciences*, *82*(2), 392–408. https://doi.org/10.1177/0020852314564308

Mesarčík, M., & Hamuľák, O. (2024). *General Data Protection Regulation: Current Challenges and Future Directions BT - E-Governance in the European Union: Strategies, Tools, and Implementation* (D. Ramiro Troitiño (ed.); pp. 117–133). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56045-3_9

Mikhalkina, E. V, Chernova, O. A., & Gozalova, A. V. (2020). *Digitalization and the Principal-Agent Problem in the Higher Education BT - Digital Future Economic Growth, Social Adaptation, and Technological Perspectives* (T. Kolmykova & E. V Kharchenko (eds.); pp. 659–665). Springer International Publishing. https://doi.org/10.1007/978-3-030-39797-5_64

Novichenko, L., Koverninska, Y., & Shysh, A. (2024). On the implementation of digital technologies in accounting and financial analysis. *Economics Finances Law*, *5*, 53–58. https://doi.org/10.37634/efp.2024.5.10

Ogbanufe, O. M., & Baham, C. (2023). Using Multi-Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret. *Information Systems Frontiers*, *25*(2), 897–916. https://doi.org/10.1007/s10796-022-10278-1

Oseni, K. O. (2024). Barriers facing e-service adopting and implementation at local environment level in Nigeria. *ArXiv Preprint ArXiv:2406.15375*. https://doi.org/10.48550/arXiv.2406.15375

Panggeso, A. G., Nirwana, & Haliah. (2024). Transparency and Accountability in Public Financial Reporting: Implementation and Challenges in the Digital Era: A Systematic Literature Review. *International Journal of Business and Applied Economics*, *3*(6 SE-Articles), 979–990. https://doi.org/10.55927/ijbae.v3i6.11875

Prasetianingrum, S., & Sonjaya, Y. (2024). The Evolution of Digital Accounting and Accounting Information Systems in the Modern Business Landscape. *Advances in Applied Accounting Research*, *2*(1 SE-), 39–53. https://doi.org/10.60079/aaar.v2i1.165

Ramos, S., & Ellul, J. (2024). Blockchain for Artificial Intelligence (AI): enhancing compliance with the EU AI Act through distributed ledger technology. A cybersecurity perspective. *International*

Cybersecurity Law Review, *5*(1), 1–20. https://doi.org/10.1365/s43439-023-00107-9

Roggenkamp, L. (2023). *Potentials of Blockchain Technology for Developing Countries BT - Chances and Challenges of Digital Management* (R. C. Geibel & S. Machavariani (eds.); pp. 77–90). Springer Nature Switzerland.

Samsor, A. M. (2021). Challenges and Prospects of e-Government implementation in Afghanistan. *International Trade, Politics and Development*, *5*(1), 51–70. https://doi.org/10.1108/ITPD-01-2020-0001

Schlegel, D., & Kraus, P. (2023). Skills and competencies for digital transformation – a critical analysis in the context of robotic process automation. *International Journal of Organizational Analysis*, *31*(3), 804–822. https://doi.org/10.1108/IJOA-04-2021-2707

Secinaro, S., Dal Mas, F., Brescia, V., & Calandra, D. (2022). Blockchain in the accounting, auditing and accountability fields: a bibliometric and coding analysis. *Accounting, Auditing & Accountability Journal*, *35*(9), 168–203. https://doi.org/10.1108/AAAJ-10-2020-4987

Sharma, S. (2020). The Future of Data Privacy. In *Data Privacy and GDPR Handbook* (pp. 407–412). Wiley. https://doi.org/10.1002/9781119594307.ch13

Shibambu, A., & Ngoepe, M. (2024). Enhancing service delivery through digital transformation in the public sector in South Africa. *Global Knowledge, Memory and Communication*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/GKMC-12-2023-0476

Sonjaya, Y. (2024). Evolving Perspectives on Public Sector Accounting Practices. *Advances in Applied Accounting Research*, *2*(2 SE-). https://doi.org/10.60079/aaar.v2i2.175

Srinivas, S., & Liang, H. (2022). Being digital to being vulnerable: does digital transformation allure a data breach? *Journal of Electronic Business & Digital Economics*, *1*(1/2), 111–137. https://doi.org/10.1108/JEBDE-08-2022-0026

Sukhwal, P. C., & Kankanhalli, A. (2022). *Agent-based Modeling in Digital Governance Research: A Review and Future Research Directions BT - Scientific Foundations of Digital Governance and Transformation: Concepts, Approaches and Challenges* (Y. Charalabidis, L. S. Flak, & G. Viale Pereira (eds.); pp. 303–331). Springer International Publishing. https://doi.org/10.1007/978-3-030-92945-9_12

Tyma, B., Dhillon, R., Sivabalan, P., & Wieder, B. (2022). Understanding accountability in blockchain systems. *Accounting, Auditing & Accountability Journal*, *35*(7), 1625–1655. https://doi.org/10.1108/AAAJ-07-2020-4713

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239–309. https://doi.org/10.1057/s41283-020-00063-2

Wirtz, B. W. (2022). *Artificial Intelligence, Big Data, Cloud Computing, and Internet of Things BT - Digital Government: Strategy, Government Models and Technology* (B. W. Wirtz (ed.); pp. 175–245). Springer International Publishing. https://doi.org/10.1007/978-3-031-13086-1_6

Yang, X. (2024). Optimizing Accounting Informatization through Simultaneous Multi-Tasking across Edge and Cloud Devices using Hybrid Machine Learning Models. *Journal of Grid Computing*, *22*(1), 12. https://doi.org/10.1007/s10723-023-09735-1