Assessment of Data Privacy Protection Framework in AI and BIM Enabled Architectural Practices in Nigeria

POPOOLA MICHEAL OLAMILEKAN[1], AKINTUNDE GLORY JOSEPH[2], AKANDE IFEOLUWA[3]
[1,2,3]*Department of Architecture, Bells University of Technology, Ota, Ogun Stat*

Abstract- ***The increasing usage of digital technologies in the construction industry result in the generation, transmission and storage of sensitive data, and this has triggered concerns over data privacy and protection in the industry, especially in developing situations where enforcement and consciousness of data protection regulations are weak. This paper evaluates data privacy and protection practices amongst construction professionals in Lagos, Nigeria to determine the existing practices, levels of awareness and compliance to data protection regulations. A quantitative research method was adopted for this study using structured questionnaires administered to a random sample of 103 construction professionals in Lagos. The collected data were analysed using descriptive statistics, relative importance index (RII) and mean score ranking to determine the extent of data protection practices, challenges associated with data protection and the major risk exposure areas. The study also determined the level of awareness of Nigeria`s Data Protection Regulation (NDPR) and few international standards (General Data Protection Regulation: GDPR). The study revealed that although there is increasing usage of digital technologies such as cloud storage, BIM, mobile apps and collaborative platforms in their designs and delivery of projects, data protection practices are sub-optimal. Password protection, antivirus software and basic encryption were found to be the most practiced methods while more advanced protocols such as rolebased access control, regular data audits and employee training were poorly adopted. The study further revealed that only 38% of respondents were aware of NDPR, and even fewer had formal data privacy policies. The study concludes that there is a huge gap in data privacy practice in Lagos construction industry driven by the level of regulatory knowledge, inadequate organisation policy framework and weak regulatory enforcement. The paper recommends training of construction professionals, development of internal data protection protocols and stronger alignment with national and international regulations. The study findings provide a strong basis for incorporating data privacy into the digitalisation agenda of Nigeria`s construction industry to ensure secure, compliant and ethical use of digital technologies in the sector.***

Indexed Terms- ***Data Privacy, NDPR, Digital Construction, Construction Professionals, Cybersecurity, BIM, GDPR***

I. INTRODUCTION

The increasing and fast adoption of Artificial Intelligence and Building Information Modeling in architectural practices has brought a lot of effectiveness, optimization and better project management to architectural practices (Akande et al., 2023). These technological advancements in the architectural sector in Nigeria have come with challenges as well. One of such challenges is data privacy breach. Information which could be very sensitive, includes project information, designs, and even personal identification data has now become an attractive target for cyber-attacks. This has raised very serious concerns of privacy, security and possible breach of confidentiality of information (Ezema & Ozioko, 2024)Raitviir and Lill (2024) define data as any information collected, processed, store transferred throughout the life cycle of an architectural project. This could be 3D models, client information, design information, financial data and even communication logs. Different types of data are essential in order for AI and BIM to analyze, forecast and automate the processes of the architectural design practice (Awe et al., 2025). The prevention of the leakage of data during the lifecycle of architectural projects is done by data

privacy (Awe et al., 2025). Architectural design practicing firms that are AI and BIM-enabled are now becoming conscious of data protection. Therefore, the increasing reliance on cloud-based storage, AI-assisted decision-making, and interconnected design platforms has now exposed architectural firms to data breaches, cyber-attacks and unauthorised data access (Tiwari, et al., 2025). The challenges underscore the urgent need for a comprehensive data privacy framework that ensures the confidentiality, integrity and security of architectural data throughout its lifestyle. Existing data protection policies and laws in Nigeria have not confronted the complexities of AI and BIM-driven architectural practice to the extent necessary (Tiwari, et al., 2025). While certain standards for global data protection, such as the General Data Protection Regulation (GDPR) and Nigeria's Data Protection Act, provide some guidance, their application within the architectural field is limited (Awe et al., 2025). There is a compelling need to assess the effectiveness of these policies, review the regulatory bodies, and determine policy modifications that can provide data privacy within Nigeria's evolving architectural paradigm.

1.1 PROBLEM STATEMENT

Application of AI and BIM in the practice of architecture has revolutionized the way designs, documentation and delivery of projects are done in Nigeria (Akande et al., 2023). These technologies, while improving operating efficiency and automation of intelligent designs, also present new risks to data security. For instance, Bala et al. (2024) reported that 76.53% of Lagos practicing architects are aware of the benefits of AI, but are also fearful of the data privacy risks that come with its use (Oke, et al., 2025). Notwith standing, although there is an increased use of the cloud for collaboration in design, and AI client interfacing, very few empirical studies have been done which investigate how AI and BIM affect data privacy in Nigerian architectural practices (Oke, et al., 2025). This gap in the industry warrants a review of the actual impact of AI and BIM on data privacy. Nigeria has also enacted data protection legislation like the Nigeria Data Protection Act (NDPA) of 2023 which applies to all personal data processing, including that used in AI systems (Asere et al., 2025). These are general legislation, and not particularly tailored to address the needs of AI and BIM facilitated architectural practices. The incidence of data breach in increasingly technologically firms is a reflection of the inefficiencies in applying these exisiting measures. For instance, the NDPA provides that organisations shall notify the data subject when they come to realise there has been a breach of personal data that is capable of exposing high risks to their privacy (Oke, et al., 2025). The absence of sectorial data policies leaves the architectural firms unable to entirely comply with secure data handling procedures. This study seeks to assess the effectiveness of existing data protection policies and procedures in architectural design environments assisted by AI technologies.. The role of regulatory bodies like National Information Technology Development Agency (NITDA) to compel data protection compliance among Nigerian architectural firms remains to be seen (Ezema & Ozioko, 2024). NITDA has initiated efforts to spur the data protection ecosystem, such as a partnership with MasterCard to train the wider ecosystem on cybersecurity and data protection (NITDA, 2022). Yet, as with industries such as finance and medicine, which possess more defined pathways of enforcement, the construction and architecture sectors have loosely regulated data systems. Without specific oversight and formal training for professionals in the AI and BIM-based design environments about standards of data protection, there would seem to be a gap requiring an investigation into the regulatory agency's role in facilitating data privacy in Nigeria's architectural industry. The existing policy landscape informing data protection in Nigeria does not capture the speedy technological revolution in architectural design practice (Ezema & Ozioko, 2024). The current legal tools are not only reactive but also lack specificity about the dynamic data streams that are the output of AI and BIM tools. For instance, while the NDPA provides the foundation for data protection, its application in architectural practice is limited as it does not address the specific issues raised by AI and BIM technologies. Without agile, sector-specific legislation, Nigerian architectural practices will remain exposed to privacy risks, underscoring the need to explore policy and regulatory reforms needed to promote improved data privacy protection in Nigeria's AI and BIM-integrated architectural practice.

1.2 AIM AND OBJECTIVES

This study aims to evaluate the effectiveness of existing data privacy protection frameworks in AI and BIM-enabled Architectural practices in Nigeria. Based on this, the objectives of the Study are:

i. To examine the impact of AI and BIM integration on data privacy.
ii. To evaluate the effectiveness of existing data protection policies and protocols in preventing data breaches.
iii. To explore the role of regulatory bodies in enforcing data protection laws in Nigeria's Architectural Sector.
iv. To recommend a comprehensive data privacy protection framework for AI and BIM enabled architectural practices in Nigeria.

II. LITERATURE REVIEW 2.1 DATA PRIVACY AND DATA PROTECTION IN ARCHITECTURAL PRACTICE

The use of digital technologies in architecture and construction in general, and in Building information Modeling (BIM) in particular, have many advantages in design but also many challenges in terms of data privacy and protection. Negri-Ribalta et al. (2024) introduced an architectural perspective of Data protection by Design to fill the gap between legal requirements and software engineering practices. Parn and Edwards (2019) argue for the needfor a border approach to cybersecurity in the built environment due to the growing trend of digital assets management and IoT technologies. Salami-Pargoo and Ilbeigi (2023) discuss cybersecurity issues in BIM environments in design, they proposed a data sharing architecture based on block-chain technology and decentralized storage to reduce the risks. These new digital tools impact on architectural practice competencies (Negri-Ribalta et al. (2024) stated in their study). Competencies. The aim of this study is to contribute to the literature by highlighting the importance of incorporating data protection measures in thearchitectural designs processes.

Concept of data privacy: Definitions and dimensions.

Data privacy can be defined as rights and expectations that individuals or organizations have over the collection, storage, usage and sharing of their personal or sensitive information (Bygrave, 2010). In the digital architectural practice, data privacy has different dimensions such as confidentiality (access to data is limited to authorized personnel), consent (request for permission to use or share data), and control (giving users or data owners the right to control how their data is used). In the AI-BIM integration, data privacy becomes an essential and inseparable aspect of the digital architectural practice since data is not only generated and used in one single platform or software, it is also shared and transferred to different collaborators which makes it an ethical and legal issue related to the professional practice as well as trust, transparency and accountability.

Distinctions between data privacy and data protection.

Data privacy and data protection are two terms that are used interchangeably but they are different (Asere et al., 2025). Data privacy is about individuals' rights regarding who can access their data and under what circumstances. Data protection, on the other hand, involves the mechanisms and tools used to secure data from unauthorised access, alteration, or destruction. In architecture practices using digital systems like AI and BIM ensuring data privacy means setting clear policies on data usage and access, while data protection involves implementing security measures such as encryption, firewalls, two-factor authentication, and secure cloud storage (França, Bonacin, & Monteiro, 2024). A breach in either domain can lead to significant reputational, legal, and financial consequences for architectural firms.

Common types of data used in architectural practice

Architectural firms manage a wide range of data types, many of which are sensitive and critical. These include client data (such as names, addresses, and budgetary information), site data (geospatial coordinates, environmental analyses, and topography), and design files (3D models, blueprints, material specifications, and schedules). With the integration of AI and BIM, this data is increasingly stored and shared across digital platforms and cloud services in collaborative environments, which exposes it to potential misuse. The sensitivity of this information makes it imperative for architectural professionals to understand data classification and apply appropriate access and protection protocols to different data types.

Risks and implications of data breaches in AI and BIM systems

AI and BIM platforms, while enhancing productivity and innovation, introduce new vectors for data breaches and cyber threats (Caetano & Leitão, 2020). Risks include unauthorised access to project models, theft of intellectual property, exposure of client and stakeholder information, and manipulation of critical design parameters. AI systems trained on poorly protected datasets may unknowingly expose private data, while BIM models often house comprehensive building information that, if accessed maliciously, can compromise building security (Zhang, 2025). For architectural firms, the implications are far-reaching: from loss of competitive advantage and project delays to legal liability and damage to client relationships. These vulnerabilities highlight the urgent need for proactive data governance strategies and compliance with global data protection regulations such as the NDPR (Nigeria Data Protection Regulation) and GDPR (General Data Protection Regulation).

2.3 EMPIRICAL REVIEW OF RELATED STUDIES

Review of related studies on research objective 1

Nitin 2023 explores the integration of BIM and AI technologies to advance various construction management processes-specifically scheduling, cost control, quality assurance, and safety management. It emphasizes the practical challenges and opportunities associated with implementing these advanced digital tools in real-world construction projects. The article primarily provides a comprehensive review of existing literature. It blends empirical case studies and recent technological advancements to illustrate how BIM and AI are being utilized in the construction environment, and case-specific implementations underpin the empirical base of the discussion. The article concludes that integrating BIM and AI offers significant potential for improving project efficiency, reducing delays and costs, and enhancing safety and quality. It also note continuous challenges such as technical complexity, lack of standardized frameworks, and resistance to change.

Nitin and Saurabh 2023 provides a foundational framework for upcoming studies and industry practices, paving the way for a more intelligent, collaborative, and efficient Architecture, engineering, and construction (AEC). This paper is to explore the integration of Building Information Modeling (BIM) with Bard, and similar generative artificial intelligence in the architecture, engineering, and construction (AEC) industry. Nitin Liladhar Rane 2024 focuses specifically on structural engineering Heating, Ventilation, and Air Conditioning (HVAC) engineering, electrical engineering, plumbing and fire protection engineering, sustainability, net zero building and green building design, Building Information Modeling (BIM), urban planning, and project management. It also made mention of Collaborative efforts between human expertise and AI capabilities are essential to unlock the full potential of generative AI in architectural engineering.

Abiodun 2024 explores the synergy between BIM and AI, examining their conceptual framework, impact on sustainability and decision-making, and the challenges associated with their integration. After a comprehensive review of recent literature and industry practice. The findings reveal that BIM and AI enhance project efficiency, resource management, decisionmaking, sustainability and stakeholder collaboration by utilizing AI's predictive analytic and automation alongside BIM's digital modeling capabilities. The study to critically examine the integration of Building Information Modeling (BIM) and Artificial Intelligence (AI) in modern infrastructure projects, evaluating their integration, impact, and future potential. The study also identified significant challenges, including issues of data interperability, high implementation costs, cybersecurity and ethical concerns. In conclusion of the article, BIM and AI hold immense potential to transform the construction and infrastructure sectors by driving innovation, sustainability, and resilience.

Ayaz 2024 investigated the challenges of implementing BIM and AI in the construction sector, by selecting and extracting the challenges, grouping them into suggesting migration strategies for major challenges. The method adopted in this research was screening and selecting relevant articles through full-text evaluation and snowballing, extracting metadata on challenges and analyzing using citation frequencies. The findings identifies some challenges to the adoption of BIM-AI in the construction sector, the research also created a map of mitigation strategies that aligned particular interventions and tactics to

combat the key challenges in every taxonomy. As a result, these challenges remain poorly understood and difficult for the construction industry to address. Gozde 2020 explores the understanding of tendency of AI in BIM research carried out in different countries and by various scholars, and to analyse and visualize the current status and relationship between AI and BIM in the AECO/FM industry.

The method used to carry out this study was Document-based citation analysis Information management, decision support systems, genetic algorithms, neural networks, knowledge-based systems, machine learning, and deep learning are the key areas where AI is being integrated with BIM research. Md-Zakaria, et. al 2024 discuss the role of Building Information Modeling (BIM) in enhancing efficiency and stability. A systematic review of the literature on the future of BIM. The findings shows that BIM integrates collaboration, efficiency, and sustainable features throughout the building's life cycle, especially with the intervention of emerging technologies like IoT, AI, and AR. Khan, et. al 2024 focused on the challenges and constraints to the integration of Building Information Modeling (BIM) and Artificial Intelligence (AI) in the construction industry by conducting a systematic literature review. A systematic review of the literature on challenges and constraints to BIM-AI integration in the construction industry was conducted. The study identifies challenges to the integration of BIM and AI in construction projects. Harish Padmanaban 2024 explores various privacy protection application contexts (e.g., encryption, DE-identification, distributed ledgers, k-anonymity). Categorization and synthesis of privacy protection methodologies based on AI-blockchain contexts and technical frameworks. The paper provides an overview of the integration of AI and block chain technologies and the emergence of privacy protection methodologies and various application contexts for privacy protection, such as data encryption, DE-identification, multi-tier distributed ledgers, and k-anonymity techniques.

Review of related studies on research objective 2
Mbah 2018 explores the pressing need for complete data protection legislation in Nigeria amid rapid digitalization and increasing cyber threats. The study reveals that Nigeria's data governance prior to 2017 was fragmented, relying on sector-specific guideline without a unified legal framework. This limitation left users vulnerable to data breaches and hindered digital trust and foreign investment. By comparing Nigeria's regulation to the GDPR and other international standards, the author highlights critical gaps such as lack of enforcement, inadequate end user rights, and poor public awareness. The article favours Protection Act, recommending explicit consent rules, and alignment with global privacy norms to safeguard Nigeria's digital economy and enhance global competitiveness. Vinh-Thong Ta et. al 202 addresses the policy and system architecture design, purpose two variants of privacy policy language and architecture description language for specifying and verifying data protection and privacy requirements. Proposing a logic-based automated verification procedure to check the conformance between policies and architectures. The approach does not cover the data subject's right to request deletion of their data. The findings propose an efficient, fully, automated verification procedure to check the conformance between a policy and an architecture.

Suhono 2025 this study explores the complexities of implementing cross-border digital identity systems and to examine how Public-Private Partnership (PPP) models can help address these challenges. The findings cover limited research on the full lifecycle of digital identity systems, including planning, implementation, and systematic evaluation and insufficient examination of societal challenges, such as digital literacy and public trust, within the context of cross-border identity frameworks. Asere 2025 examine the impact of data privacy regulations, such as Nigeria's Data Protection Regulation (NDPR) and the African Union's Convention on Cyber Security and Personal Data Protection. The findings concluded that data privacy regulations have improved organizational cybersecurity practices in Nigeria, but enforcement and resource challenges remain and also need for more comparative studies exploring enforcement challenges of data privacy regulations across different African jurisdictions.

Geraldine 2018 evaluate the effectiveness of Nigeria's data protection framework and propose policy recommendations to enhance data governance in Nigeria by using a qualitative research approach which

he concluded that regulatory agencies had limited authority to enforce compliance, allowing many businesses to ignore privacy guidelines without consequences and Absence of legal rights for consumers over their personal data, allowing businesses to collect and use data without explicit consent. Michael 2020 explores data protection and compliance in Nigeria, identify the issues and challenges, and compare it to other countries and literature review was implemented during this research. The paper argues that data protection and privacy are practically strange to the Nigerian society, with data subjects generally unaware of their privacy rights, leading to high levels of data breaches and abuse. Lack of prioritization of data protection and privacy, particularly in developing countries like Nigeria, despite the increasing number of data breaches globally.

Review of related studies on research objective 3
Oluwatosin 2023 analyse the innovations introduced in the Nigeria Data Protection Act 2023 and identify areas for improvement. Which identifies areas that require further clarification or improvement, such as the definition of "data controllers/processors of major importance" and the independence of the Data Protection Commission. Misbau 2022 examines the powers of the National Information Technology Development Agency (NITDA) to enforce data protection laws in Nigeria, specifically the NITDA Act and the Nigeria Data Protection Regulation (NDPR). It also identifies areas that require further clarification or improvement, such as the definition of "data controllers/processors of major importance" and the independence of the Data Protection Commission. Leon 2023 examine the challenges experienced in implementing data protection laws. Method involved a review of existing literature and published reports accessed through online journals and libraries. Findings shows that regulatory authorities lack the resources to properly monitor and inspect compliance with data protection laws. Adams and Yumei 2020 extend a previous architecture for enforcing privacy when users submit personal data to websites, by strengthening the enforcement portion of the architecture through the use of IBE technology and third-party auditing. The research proposes using enterprise architecture patterns to integrate data protection and privacy regulations, with a focus on the rights of data subjects.

Review of related studies on research objective 4
Sarah et al 2024 provides a thorough analysis of data privacy legislation, compliance rates, enforcement strategies, and related issues in African countries. Systematic review methodology to comprehensively analyze and synthesize existing research on data privacy laws and compliance. The findings shows majority of African countries have comprehensive data privacy laws, while a few lack dedicated legislation and face compliance challenges. Edward 2018 describe and analyze the implications of the EU General Data Protection Regulation (GDPR) for international scientific research that involves the processing of participants' personal data. However, there are concerns that the GDPR's implementation may not be harmonized across Europe, potentially leading to regulatory fragmentation. The need for further steps to guide researchers, improve regulatory harmonization, address a culture of caution around compliance, and enhance responsible data sharing to facilitate scientific progress. Vinh-Thong et al 2021 address the policy and system architecture design, propose two variants of privacy policy language and architecture description language for specifying and verifying data protection and privacy requirements. The paper proposes an efficient, fully automated verification procedure to check the conformance between a policy and an architecture.

Oluwabunmi et al 2024 examine the current landscape of data privacy and security within the context of environmental research, and to identify and analyze the challenges, developments, and strategic implications associated with safeguarding sensitive environmental data. The findings shows that there is a growing emphasis on robust data governance frameworks driven by advancements in digital technologies and the global diffusion of regulations like the GDPR. Ghorashi, et al 2023 examine the privacy protection challenges in data sharing between organizations and third-party entities, focusing on changing collaborations in the digital age. Exploration of industrial privacy frameworks, such as National Institute of Standard Technology NIST and Five Safes, and their comprehensive procedural and technical guidance. The study examines the privacy challenges

in data sharing between organisations and thirdparty entities in the digital age. The study explores industrial privacy frameworks like NIST and Five Safes, which provide comprehensive procedural and technical guidance, bridging the gap between legal mandates and practical applications.

III. RESEARCH METHODOLOGY

3.1 INSTRUMENT OF DATA COLLECTION

The study employed s structured questionnaire as the primary research instrument, designed to capture both normal and ordinal data, which are suitable for the study.

Questionnaire

The primary instrument for data collection was a structured questionnaire based on the research questions. The questionnaire is divided into four sections:

i. Section A: Demographic information
ii. Section B: Impact of AI and BIM in data privacy
iii. Section C: Effectiveness of existing data protection policies
iv. Section D: Role of regulatory bodies
v. Section E: Policy and regulatory recommendations

A 5-point-like scale is used for sections B to E, ranging from;
1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree

The scale above is widely accepted in social science research for measuring attitudes and perceptions. The questions were designed to ensure clarity and eliminate ambiguity.

The study population

The target population comprises licensed architectural design practicing firms in Lagos state, Nigeria. Lagos is selected due to its concentration of architectural firms and high technology adoption rate. According to the Architects Registration Council of Nigeria (ARCON) registers, Lagos state has 349 firms and remains the state with the highest cluster of firms in Nigeria.

IV. RESULTS AND DISCUSSION

Professional Affiliation of Respondents

The professional distribution reveals that a majority of the respondents, approximately 59.02%, are architects. This is a critical observation as it suggests that the study is strongly anchored in the architectural domain—the core area of inquiry. Other respondents include engineers (22.95%), IT specialists (12.30%), and a minimal representation from builders, interior designers, project managers, and quantity surveyors (each constituting less than 1%). The concentration of architects and engineers implies that the perspectives gathered are largely from professionals who are either direct users or primary collaborators in AI and BIM-based design environments. The presence of IT specialists, although smaller, is significant as they contribute expert insights into the technical aspects of data privacy and system vulnerabilities.

Years of Experience of Respondents

Regarding years of professional experience, the data indicates a well-balanced range among participants. About 32.79% of respondents have between 5 to 10 years of experience, another 32.79% have less than 5 years, 26.23% have between 11 to 15 years, while 8.20% possess over 15 years of professional engagement. This spread demonstrates that the sample comprises both emerging professionals and seasoned practitioners, providing a comprehensive view of how data privacy issues are perceived across varying career stages. Notably, the significant proportion of early- to mid-career professionals suggests a cohort likely to be more familiar with evolving digital technologies such as AI and BIM, potentially influencing their awareness and assessment of data privacy frameworks.

Experience with AI or BIM in Architectural Practice

Furthermore, a striking 84.43% of respondents indicated that they have used either AI or BIM technologies in their architectural practice. This high level of adoption underscores the relevance and timeliness of the research, affirming that most participants are speaking from practical experience. It also highlights the increasing penetration of digital technologies within Nigeria's architectural sector, thus justifying the need to investigate data privacy concerns within this context. The demographic profile reflects a knowledgeable and professionally diverse group, with

a strong inclination toward architectural practice and digital technology adoption. This enhances the validity of the research findings and supports their application in formulating a robust and contextually appropriate data privacy protection framework for AI and BIM-enabled architectural practices in Nigeria.

Table 4.1: Professional Affiliation of Respondents

Profession	Frequency	Percentage (%)
Architect	72	59.02
Engineer	28	22.95
IT Specialist	15	12.30
Builder	1	0.82
Building Contractor	2	1.64
Interior Designer	1	0.82
Project Manager	2	1.64
Quantity Surveyor	1	0.82
Total	122	100.00

Table 4.2: Years of Experience of Respondents

Years of Experience	Frequency	Percentage (%)
Less than 5 years	40	32.79
5 – 10 years	40	32.79
11 – 15 years	32	26.23
Above 15 years	10	8.20
Total	122	100.00

Table 4.3: Experience with AI or BIM in Architectural Practice

Usage of AI/BIM	Frequency	Percentage (%)
Yes	103	84.43
No	19	15.57
Total	122	100.00

Impact of AI and BIM Integration on Data Privacy

In addressing the first research objective, to examine the impact of AI and BIM integration on data privacy in architectural practices in Nigeria, the study utilised descriptive statistical analysis to evaluate various dimensions of how these technologies influence data privacy risks and operational efficiencies. The results indicate a strong perceived impact of AI and BIM integration on efficiency improvement, with a mean score of 3.93 and a standard deviation of 0.95. This suggests that respondents generally acknowledge the significant benefits that AI and BIM tools bring to architectural workflows, particularly in terms of speed, coordination, and automation of design processes. The relatively low standard deviation points to a strong consensus among participants on this matter.

However, while efficiency is enhanced, the data also points to several privacy and security concerns that emerge with increased digital integration. For instance, data breach risk was rated at a mean of 2.98 with a standard deviation of 1.21, indicating a moderate level of concern, with some variability in perceptions. Similarly, cloud storage vulnerability, which reflects apprehension about storing sensitive architectural and client data on third-party servers, recorded a mean of 3.20. This is marginally higher than the midpoint and suggests that participants recognise inherent risks associated with cloud-based solutions, which are integral to AI and BIM ecosystems. The issue of unauthorised data accesses also emerged with a mean of 3.02, further emphasising concerns over how architectural data may be exposed or exploited, either internally or externally. This aligns with the growing awareness of cyber threats in digitalised design environments where access control and identity management become critical.

Lastly, the composite indicator for data privacy challenges recorded a mean of 2.86, the lowest among the variables under this objective. Although slightly below the midpoint, this score still indicates a perceptible level of concern. It may reflect varying degrees of understanding or prioritisation of privacy issues among practitioners, some of whom might be more focused on operational efficiency than on the nuanced implications of data privacy. In synthesis, the findings suggest a dual reality: while AI and BIM integration is widely recognised as transformative in improving architectural practice efficiency, it concurrently introduces moderate concerns about data privacy and security. This tension underscores the importance of implementing robust privacy protection measures alongside technological adoption, especially as the Nigerian architectural sector continues to digitalise. The results affirm the necessity of addressing privacy risks not only through technical safeguards but also through organizational and regulatory interventions, which are explored further in the subsequent research objectives.

Table 4.4: Impact of AI and BIM Integration on Data Privacy

Variable	Mean	Standard Deviation
Efficiency Improvement	3.93	0.95
Data Breach Risk	2.98	1.21
Cloud Storage Vulnerability	3.20	1.15
Unauthorised Data Access	3.02	1.24
Data Privacy Challenges	2.86	1.21

Effectiveness of existing data protection policies

In pursuit of the second objective, to evaluate the effectiveness of existing data protection policies and protocols in preventing data breaches in AI and BIM-enabled architectural practices in Nigeria, the study employed descriptive statistical analysis to assess practitioners' perceptions across various institutional, national, and international frameworks and practices. The results reveal a moderately positive perception of existing data protection mechanisms. Among the variables assessed, AI security measures recorded the highest mean score of 3.52, with a standard deviation of 1.05. This indicates that respondents believe current security protocols specific to AI tools offer a relatively effective line of defence against data vulnerabilities. The variability in responses suggests a degree of inconsistency in how these measures are implemented or understood across different firms. Closely following this was cybersecurity training, with a mean of 3.49 and a standard deviation of 0.94. This finding highlights a growing recognition of the importance of human-centric interventions, such as capacity building and staff sensitisation, to mitigate cybersecurity risks. It suggests that firms providing regular training are seen as better positioned to handle potential data breaches in their digital workflows. The firm-level data policies also scored relatively well, with a mean of 3.40. This implies that, to a moderate extent, architectural firms have internal policies that guide data usage, access control, and information handling. However, the effectiveness of these policies may vary significantly across firms, particularly between larger, well-resourced organisations and smaller practices with limited technical infrastructure. Data encryption, a fundamental technical measure for ensuring data confidentiality and integrity, had a mean of 3.34, indicating a fair but not universal adoption of this security layer. Given that encryption is essential for protecting sensitive architectural data, especially when transmitted or stored on cloud platforms, the moderate score suggests room for improvement in its consistent application.

Regarding external legal frameworks, the applicability of the General Data Protection Regulation (GDPR) in the Nigerian context received a mean score of 3.30. This points to a partial alignment with international data privacy standards, though the result may also reflect ambiguities or challenges in implementing GDPR principles within Nigeria's legal and institutional realities. Finally, the effectiveness of Nigeria's Data Protection Act (NDPA) was rated the lowest among the variables, with a mean of 3.16. This suggests a general perception that national data protection laws, while present, are not yet fully effective in practice. The relatively low score highlights possible gaps in enforcement, awareness, or integration of these laws into the workflows of AI and BIM-enabled architectural firms. The findings suggest that while there is a foundational layer of data protection policies and practices within Nigeria's architectural sector, these mechanisms are not uniformly effective or comprehensively adopted. The moderate scores across all indicators underscore the need for strengthened regulatory compliance, more robust internal policies, and enhanced training programs to ensure that data protection protocols can effectively prevent breaches in the increasingly digitalised architectural landscape.

Table 4.5: Effectiveness of Existing Data Protection Policies and Protocols

Variable	Mean	Standard Deviation
NDPA Effectiveness	3.16	0.80
GDPR Applicability	3.30	0.94
Firm Data Policies	3.40	0.98
Data Encryption Use	3.34	0.99
Cybersecurity Training	3.49	0.94
AI Security Measures	3.52	1.05

Role of Regulatory Bodies in Enforcing Data Protection Laws

The third objective of the study sought to explore the role of regulatory bodies in enforcing data protection laws within AI and BIM-enabled architectural practices in Nigeria. Descriptive statistical analysis was employed to assess respondents' perceptions of various national institutions and their enforcement effectiveness, as well as the level of regulatory awareness within architectural firms. The findings reveal a generally moderate perception of regulatory effectiveness, suggesting that while institutional mechanisms for data protection are in place, their enforcement and impact remain limited or uneven. The variable Privacy Law Enforcement received the highest mean score of 3.34, with a standard deviation of 1.03, indicating that there is a general belief among professionals that data privacy laws exist and are being enforced to some extent. However, the relatively high standard deviation also points to divergent experiences or awareness levels regarding how consistently these laws are applied across the industry. NITDA Enforcement Effectiveness was rated at a mean of 3.31, suggesting a fair level of confidence in the National Information Technology Development Agency's efforts to enforce data protection guidelines. NITDA's role as a central regulatory authority for data protection in Nigeria appears to be recognized, yet the score implies that its visibility and impact in the architectural sector may still be evolving.

The variable Firm Awareness of Regulations recorded a mean score of 3.26, reflecting a moderate level of awareness among architectural practices regarding existing data protection regulations. This suggests that while many firms are aware of their responsibilities under national data laws, this awareness may not be widespread or deeply embedded across the sector, particularly among smaller or less digitally advanced practices. ARCON Data Privacy Guidance, representing the efforts of the Architects Registration Council of Nigeria to offer sector-specific guidance, received a mean score of 3.16. This relatively lower score may indicate a perceived lack of proactive engagement or tailored regulatory communication from ARCON on data privacy issues in relation to AI and BIM integration. It points to a potential gap in the regulatory ecosystem, where general data protection mandates exist but are not sufficiently contextualized for architectural practice.

Lastly, Government Monitoring Effectiveness yielded the lowest score, with a mean of 3.14 and a standard deviation of 0.98. This reflects a perception that government oversight mechanisms are limited in scope or effectiveness when it comes to monitoring data practices within the architectural profession. The score suggests that while regulatory structures are in place, their real-time or practical enforcement may be lacking. In summary, the data indicates that while regulatory bodies such as NITDA and ARCON are recognized for their roles in establishing data protection frameworks, the enforcement and contextual relevance of these regulations in architectural practice remain areas of concern. There is a clear need for more targeted regulatory guidance, increased institutional engagement with the architectural sector, and improved mechanisms for monitoring and enforcement to ensure the effective protection of data in an era of growing AI and BIM integration.

Table 4.6: Role of Regulatory Bodies in Enforcing Data Protection Laws

Variable	Mean	Standard Deviation
NITDA Enforcement Effectiveness	3.31	0.90
ARCON Data Privacy Guidance	3.16	0.92
Government Monitoring Effectiveness	3.14	0.98
Privacy Law Enforcement	3.34	1.03
Firm Awareness of Regulations	3.26	0.98

Policy and Regulatory Changes Needed for Improved Data Privacy Protection

In addressing the fourth research objective, namely, to recommend a comprehensive data privacy protection framework for AI and BIM–enabled architectural practices in Nigeria, the descriptive statistics reveal practitioners' strong endorsement of several key policy and regulatory interventions. The highest mean score of 3.80 (SD = 0.92) for "Stricter Breach Penalties"

underscores a clear sentiment that imposing more severe sanctions for unauthorized disclosures or cyber-incidents would serve as an effective deterrent and encourage firms to prioritize data protection measures. Almost equally compelling is the call for explicit "NDPA AI-BIM Regulations," which registered a mean of 3.79 (SD = 0.92), indicating that respondents perceive a need for the National Data Protection Act to be amended or supplemented with provisions that directly address the unique risks introduced by AI algorithms and BIM platforms. Equally significant is the endorsement of a formal "Cybersecurity Framework Architecture" for the sector, which achieved a mean of 3.77 (SD = 0.94). This finding suggests that respondents favour the development of structured, standardised protocols, potentially modelled on international best practices, to guide architectural firms in implementing layered security controls, incident response plans, and continuous monitoring mechanisms. Parallel to this, "Data Security Training" garnered a mean of 3.61 (SD = 0.99), reflecting the conviction that enhancing employees' competencies through regular, targeted training is indispensable for sustaining a culture of privacy awareness and for reducing human-factor vulnerabilities that often precipitate breaches.

Lastly, while "Mandatory AI Security" measures received the lowest mean among the five indicators (mean = 3.60, SD = 0.92), the relatively high score still signals broad agreement that enforcing baseline security requirements for AI tools, such as algorithmic auditing, model-drift detection, and secure development lifecycles, should form an integral component of any holistic data privacy framework. Collectively, these results indicate that practitioners in Nigeria's architectural sector advocate for a multifaceted policy agenda: one that combines legislative refinement, punitive deterrents, formalised technical architectures, and humancentric training to safeguard sensitive design and client data in the era of AI and BIM integration.

Table 4.7: Policy and Regulatory Changes for Improved Data Privacy Protection

Variable	Mean	Std Deviation
NDPAAIBIMRegulations	3.79	0.92
StricterBreach Penalties	3.80	0.92
Mandatory AI Security Measures	3.60	0.92
Data Security Training	3.61	0.99
Cybersecurity Framework Architecture	3.77	0.94

CONCLUSION

The findings of the study revealed that the integration of AI and BIM in architectural practices has bought about a significant transformation in the Nigerian construction industry, these technologies has enhance the accuracy, smartness and efficiency of design processes. However, the study found that the existing data protection policies and protocols in many Nigerian architectural firms are not enough. While some firms have acquire basic cybersecurity measures such as password protection and structured data protection. Many firms do not fully comply with the Nigeria Data Protection Regulation (NDPR), and awareness of international best practices remains limited. the study proposes the development of a comprehensive data privacy protection framework tailored to the unique needs of AI and BIM-enabled architectural practices in Nigeria. Data privacy is an ethical issues under AI and BIM that needs to be resolved and looked into. There is need for us to develop a framework or guideline to protect privacy, that is the purpose for carrying out this research to protect people's privacy. It is not something that is common here. Based on existing literature in the field of architecture under the use of AI and BIM it has yet to look into the data protection framework yet, this research establish that framework or guideline for data protection framework in AI and BIM-enabled architectural practices in Nigeria.

REFERENCES

[1] Agbali, M. A., Dahiru, G., Olufemi, I. A., & Kashifu, O. V. (2020). Data Privacy and Protection: The Role of Regulation and

Implications for Data Controllers in Developing Countries. *Information and Communication Technologies for Development*, 1-12.

[2] Agency, N. I. (2022). *Data Protection & Cyber Security: NITDA, MasterCard Partner to Improve Ecosystem.* Abuja: National Information Technology Development Agency.

[3] Akande, I., Alagbe, O. T., Adebayo, O. A., Olaosun, S., & Oyedele, I. O. (2023). Prospects And Challenges Of Emerging Technologies In Architectural Design Practice Within The Nigerian Context. *Journal of Namibian Studies*, 33.

[4] Akash, P. (2025). *BIM Levels Explained.* East Hartford: United BIM.

[5] Asere, G. F., Adenomon, M. O., Aimufua, G. I., & Ibrahim, U. (2025). The Effects of Data Privacy Regulations on Cybersecurity Practices in Nigeria and Africa. *Journal of Cyberspace Studies*, 1-24.

[6] Awe, M., Malhi, A., Budka, M., Mavengere, N., & Dave, B. (2025). Towards 4D BIM: A Systematic Literature Review on Challenges, Strategies and Tools in Leveraging AI with BIM. *Buildings*, 15(7), 1072.

[7] Bygrave, L. A. (2010). Privacy and data protection in an international perspective. *Scandinavian studies in law*, 56(8), 165-200.

[8] Caetano, I., & Leitão, A. (2020). Architecture meets computation: an overview of the evolution of computational design approaches in architecture. *Architectural Science Review*, 63(2), 165-174.

[9] Ciranka, S., & Van den Bos, W. (2019). Social influence in adolescent decision-making: A formal framework. *Frontiers in psychology*, 10, 1915-1921.

[10] Ezema, A. O., & Ozioko, M. V. (2024). The Importance of Governance in Safeguarding Privacy and Security in Nigeria's Technology Industry: A Legal Review . *Nnamdi Azikiwe University Journal of Private and Property Law*, 1(1), 138-151.

[11] França, R. P., Bonacin, R., & Monteiro, A. C. (2024). An Overview of Data Privacy and Security in Cloud Platforms: Exploring the Intersection of Digital Technologies Currently. *Digital Cultural Heritage*, 21-39.

[12] Israel, O., & Chukwuemezie, C. E. (2021). An Examination of the Legal Framework for Data Privacy and Protection in Nigeria. *Social Science Research Network*, 23-25.

[13] Koutamanis, A., Dainty, A., Kvan, T., & Turk, Ž. (2021). The enigma of BIM. *Architecture, Structures and Construction*, 1-9.

[14] Negri-Ribalta, C., Lombard-Platet, M., & Salinesi, C. (2024). Understanding the GDPR from a requirements engineering perspective—a systematic mapping study on regulatory data protection requirements. *Requirements Engineering*, 29(4), 523-549.

[15] Nermen, M. M., & Nevine, G. G. (2024). Artificial Intelligence in Architecture: Integration into Architectural Design Process. *Engineering Research Journal*, 181.

[16] Oke, A. E., Adekunye, O. J., Adeosun, F. E., Aliu, J., Akanni, P. O., Aghimien, D., & Aigbavboa, C. O. (2025). Assessment of the challenges of integrating cyber-physical systems in Nigerian construction. Engineering. *Engineering, Construction and Architectural Management.*, 33.

[17] Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management*, 26(2), 245-266.

[18] Raitviir, C. R., & Lill, I. (2024). Conceptual Framework of Information Flow Synchronization throughout the Building Lifecycle. *Buildings*, 14(7), 2207.

[19] Saad, S., Haris, M., Ammad, S., & Rasheed, K. (2024). AI-assisted building design. *AI in material science*, 143-168.

[20] Salami-Pargoo, N., & Ilbeigi, M. (2023). A scoping review for cybersecurity in the construction industry. *Journal of Management* in *Engineering*, 39(2), 03122003.

[21] Salawu, R., Shamsuddin, A., Bolatitio, S., & Masibo, S. (2023). Theoretical and conceptual frameworks in research: Conceptual

clarification. *European Chemical Bulletin*, 12(12), 2103-2117.

[22] Sürücü, L., & Maslakci, A. (2020). Validity and reliability in quantitative research. *Business & Management Studies: An International Journal*, 8(3), 2694-2726.

[23] Tellios, A., Koulali, P., & Valsamidou, K. (2024). Designing Tomorrow: AI and the Future of Architectural Design Process. *Interdisciplinary Journal of Architecture And Built Environment*, (27), 22-25.

[24] Tiwari, A., Masilamani, M., Rao, T. S., Zope, S., Deepak, S. A., & Karthick, L. (2025). Shaping the Future: Emerging Trends and Strategic Predictions in Big Data and AI. *AI and the Revival of Big Data*, 125-154.

[25] Zhang, X. (2025). BIM model generation and protection: an automated solution under deep learning and differential privacy. *Evolutionary Intelligence*, 18(1), 29.