Journal of Public Management and International Relations (JPMIR)

ISSN: 3134-8769

Volume 1, Number 3, July 2026

Pp 296-315

Digital Security and Land Protection Methods in Obafemi Awolowo University, Ile-Ife, Nigeria

***Kazeem Oyedele Lamidi**
Department of Local Government and Development Studies
Faculty of Administration
Obafemi Awolowo University
Ile-Ife, Nigeria
akandekande@oauife.edu.ng
akandekande@gmail.com
https://orcid.org/0000-0002-0434-8990

Hammed Adetola Adefeso
Department of Local Government and Development Studies
Faculty of Administration
Obafemi Awolowo University
Ile-Ife, Nigeria
haadefeso@oauife.edu.ng
https://orcid.org/0000-0003-2908-5119

Oluwatobi Ojo Adeyemi
Department of Local Government and Development Studies
Faculty of Administration
Obafemi Awolowo University
Ile-Ife, Nigeria
ooadeyemi@oauife.edu.ng
https://orcid.org/0000-0001-8889-0340

Jimoh Akanji Hassan
Department of Computer Science and Engineering
Faculty of Computing Science
Obafemi Awolowo University
Ile-Ife, Nigeria
jahassan@oauife.edu.ng

*Corresponding Author

DOI: https://doi.org/10.51415/jpmir.v1i3.1759

Published by the Department of Public Management, Law and Economics
Durban University of Technology, Pietermaritzburg, South Africa

Abstract

This study examines digital security and land protection methods at Obafemi Awolowo University (OAU), Ile-Ife, Nigeria. Land encroachment and urban expansion pose significant challenges to protecting institutional land assets. Despite the growing relevance of digital technologies in land governance, existing protection measures remain largely reactive and insufficient for addressing technologically sophisticated and spatially dispersed threats. This study addresses this gap by examining the effectiveness of digital security and land protection methods at OAU. Guided by systems theory and socio-technical systems perspectives, the study conceptualises land protection as an interconnected system involving digital infrastructure, governance structures, human capacity, and environmental factors. The study evaluates existing digital security measures, identifies institutional and technological constraints, and proposes strategies for improving land protection through integrated digital governance. A qualitative research design was employed. Data were collected through in-depth interviews with 20 purposively and stratified selected stakeholders from the ICT Unit, Physical Planning Unit, Legal Unit, and Security Department. The data were analysed using content analysis. Findings reveal that digital security technologies at OAU are underdeveloped, poorly integrated, and inadequately aligned with land governance processes. GIS applications are mainly used for internal planning, surveillance is concentrated within core campus areas, and digital land records lack adequate cybersecurity protection. Institutional fragmentation, weak collaboration, and limited technical capacity further reduce effectiveness. The study proposes an integrated digital land management framework and concludes that effective land protection requires alignment among technology, governance structures, and human actors.

Keywords: Digital Security; Land Protection; Geographic Information Systems (GIS); Land Encroachment; Cybersecurity; Integrated Land Management

Introduction

Obafemi Awolowo University (OAU), Ile-Ife, serves as a compelling case study in the Nigerian higher education context due to its expansive land holdings and complex operational environment. As one of Nigeria's premier federal universities, OAU manages vast physical and digital infrastructures, encompassing academic, administrative, and residential functions. In recent years, the University has faced increasing threats from unauthorised land encroachments, illegal mining activities, and community claims on university land, reflecting broader challenges experienced by higher education institutions across Nigeria (Balogun, 2019). These encroachments not only jeopardise physical land boundaries but also threaten institutional assets, disrupt campus operations, and pose significant risks to the university's financial, infrastructural, and reputational integrity. Land protection is not only an environmental and legal imperative but also an institutional necessity. The ecological rationale for land conservation is clear: preserving natural systems enhances carbon sequestration, maintains watershed functions, supports soil conservation, and safeguards diverse habitats (Daily, 1997; Brauman et al., 2007; Kumar, 2012; Watson et al., 2014). These functions are particularly relevant to OAU, where protected lands support research, teaching, and recreation, while contributing to the broader environmental quality of the campus. Beyond ecology, land protection addresses market failures in land allocation. Private landowners often underprovide socially beneficial land uses such as forests, agricultural lands, and managed timberlands because many of the associated benefits accrue to the public rather than the individual owner (Angelsen, 2010; Tietenberg & Lewis, 2016). As a public institution, OAU can strategically allocate land for purposes that maximise social, academic, and environmental value, correcting these market inefficiencies.

Moreover, protected lands enhance the amenity value of OAU, making the university an attractive destination for students, staff, researchers, and visitors. Research indicates that the presence of attractive environmental and social amenities can drive migration and subsequent economic growth, with in-migration often preceding employment creation (Rasker et al., 2013; Wu & Plantinga, 2003; Chen et al., 2016; Greenwood & Hunt, 1984; Nelson, 1999; Lorah & Southwick, 2003; Baskett et al., 2013). Amenity-driven growth has been identified as a critical factor in the sustained positive impacts of land protection in various contexts, including the Western United States and northeastern states, where environmental amenities are linked to economic expansion and community well-being (White & Hanink, 2004).

The increasing pressures on OAU's land holdings are compounded by urbanisation and the digitisation of land management systems in Nigeria. Surrounding communities are often motivated to reclaim portions of institutional land as urban expansion encroaches on university territories (Adeyinka, 2024). This creates additional challenges for institutions like OAU, which must safeguard their physical and digital assets while maintaining positive town-gown relations. The sophistication and persistence of encroachment activities, including unauthorised settlement, illegal mining, and pressure from host community representatives, have highlighted the limitations of relying solely on traditional physical security measures. The University's internal security personnel are increasingly challenged by these activities, underscoring the need for a technologically integrated approach to land protection.

While previous studies have examined land tenure, encroachment, and protection challenges in Nigerian universities (Ugando, Egolum & Sado, 2023), few have focused on the role of digital security in safeguarding institutional lands. In OAU, physical monitoring of land boundaries is often insufficient, with limited application of geospatial documentation, surveillance technologies, and cybersecurity frameworks. The absence of an integrated digital-physical security system exacerbates the vulnerability of the university's land assets, leaving the institution exposed to financial, infrastructural, and reputational risks (Akinola et al, 2019; Zikder, Aksu & Uluagac, 2020; Cheng & Wang, 2022; Ugando, Egolum & Sado, 2023).

Globally, Geographic Information Systems (GIS), digital surveillance, and cybersecurity tools have become integral to land management, providing precise geospatial mapping, real-time monitoring, and data-driven decision-making capabilities (Taiwo et al, 2024). Yet, OAU has not fully developed integrated digital strategies to mitigate land encroachment risks. Coordination between digital and physical security systems is minimal, while traditional land management practices remain outdated. This combination of factors increases the university's susceptibility to encroachment and illegal land use, emphasising the need for an innovative, technology-driven approach. The study, therefore, proposes investigating digital security and land protection methods at Obafemi Awolowo University to design an integrated framework that combines GIS technologies, surveillance systems, and cybersecurity protocols. Such an approach aims to enhance the university's capacity to monitor, secure, and manage its land holdings effectively. By leveraging multidisciplinary technologies, OAU can strengthen legal and institutional protection of its land assets, prevent unauthorised access, and optimise land use in alignment with both conservation and development goals.

The study aims to explore digital security and land protection methods in Obafemi Awolowo University, with a view to proposing a comprehensive, integrated framework for improved land security. This study addresses a critical gap in existing research on Nigerian universities. It emphasises the need for proactive, technologically advanced measures to safeguard institutional assets in the face of increasing urbanisation, community pressures, and the growing sophistication of encroachment activities. In doing so, the study highlights the potential of digital security to complement traditional land management practices, ensuring that OAU's land remains protected for ecological sustainability, academic use, and long-term institutional development. The study thus provides a timely and necessary contribution to understanding how digital innovation can reinforce traditional land management practices in Nigerian higher education institutions, ensuring the university's land resources remain secure, legally protected, and sustainably managed for future generations.

Context of Land Protection in Obafemi Awolowo University

Land encroachment in Nigerian public institutions is often attributed to poor documentation, limited legal enforcement, and lack of surveillance technologies (Olawoyin & Lamidi, 2019). According to Ugando, Egolum & Sado (2023), most universities operate with outdated land tenure records, leaving them vulnerable to illegal occupation and disputes. GIS technology has been recognised as a viable solution for spatial planning and land demarcation (Adeyinka, 2024), yet many institutions lack the capacity to utilise resources for full implementation. Cybersecurity challenges in Nigerian universities stem from poor infrastructure, low

cybersecurity literacy, and inconsistent policy implementation (Akinola et al, 2019). The increasing reliance on digital platforms for academic, administrative and financial transactions has exposed universities to phishing, ransomware, and unauthorised access. Despite the availability of advanced tools like firewalls, Intrusion Detection Systems (IDS), and encryption protocols, their adoption in many Nigerian universities remains minimal (Cheng & Wang, 2022). The convergence of geospatial technology and digital security presents a promising frontier for institutional protection. Integrated systems that employ real-time surveillance, biometric access control, and network security protocols have shown effectiveness in other sectors (Zikder, Aksu & Uluagac, 2020). However, there is limited empirical research applying these systems holistically within Nigerian universities. This study contributes by proposing a model that integrates GIS-based land monitoring with robust digital infrastructure security.

Land protection, whether public or private, plays a critical role in sustaining ecological integrity by preventing the conversion of natural systems into intensive, developed uses. Within the context of Obafemi Awolowo University (OAU), land conservation preserves the university's green spaces, forested areas, and water catchments, yielding ecological benefits such as carbon sequestration, maintenance of watershed functions, soil conservation, and the protection of diverse habitats for both flora and fauna (Daily, 1997; Brauman et al., 2007; Kumar, 2012; Watson et al., 2014). These ecological functions are particularly valuable in a university setting, where protected lands support research, teaching, and recreation while enhancing the campus environment for staff, students, and visitors.

Beyond ecological benefits, land protection addresses a fundamental market failure in land use allocation. Private markets typically underprovide land for socially beneficial purposes such as natural forests, agricultural lands, or managed timberlands because many of the benefits of such lands accrue to the public at large rather than individual landowners. When private values and market transactions determine land use, less land is devoted to socially desirable purposes than would occur if land use were determined collectively based on social value (Angelsen, 2010; Tietenberg & Lewis, 2016). As a public institution, OAU mitigates this market failure by conserving and managing land in a way that prioritises ecological, educational, and social value over purely financial returns.

Despite the clear ecological and economic rationale for land protection, it inherently restricts intensive land conversion, including housing, commercial development, and other revenue-generating uses. Critics of land protection often focus on these limitations, highlighting potential losses in tax revenue or economic opportunities, and argue that such restrictions may be incompatible with economic growth, especially in areas where employment opportunities are limited (Lewis et al., 2007; Lilieholm, 2007; Daily, 2017; Davenport, 2017). Within the OAU campus, similar tensions may arise when the demand for student hostels, staff housing, or commercial facilities intersects with the university's conservation priorities.

Proponents of land protection, however, emphasise its broader contributions to local economic and social development. Protected lands provide ecosystem services, including pollination, flood regulation, watershed maintenance, and sustainable forest products that support economic activity while preserving environmental quality (Kurtz, 2010). Additionally, land protection can generate employment opportunities directly or indirectly associated with conservation, such as campus maintenance, research support, landscaping, agricultural production, and eco-tourism initiatives (Dixon & Sherman, 1990; Philips, 1998; Kurtz, 2010; Thomas et al., 2015). The economic effects of such employment are amplified when employees and visitors spend locally, creating a multiplier effect as local producers purchase inputs from other local businesses or reinvest income within the community (Thomas et al., 2015).

Land protection also enhances the amenity value of OAU, making the university a more attractive destination for students, staff, researchers, and visitors. Amenity-related growth is an increasingly recognised driver of regional development, where the presence of attractive environmental and social amenities can stimulate migration and subsequent economic growth (Rasker et al., 2013; Wu & Plantinga, 2003; Chen et al., 2016; Greenwood & Hunt, 1984; Nelson, 1999; Lorah & Southwick, 2003; Baskett et al., 2013). In similar contexts

in the United States, protected lands have been shown to generate sustained positive economic impacts through enhanced local and regional attractiveness (Rasker et al., 2013; Chen et al., 2016). Research in other regions, such as Northeastern U.S. states, also demonstrates a strong association between environmental amenities and economic growth (White & Hanink, 2004).

Land Encroachment and Cybersecurity Vulnerabilities in Nigerian Universities: Toward an Integrated GIS-Based Protection Framework

Land encroachment has emerged as a persistent challenge confronting public institutions in Nigeria, particularly universities with expansive land holdings. Existing literature attributes this phenomenon largely to weak land administration systems, poor documentation practices, limited legal enforcement, and the absence of effective surveillance technologies. Olawoyin and Lamidi (2019) observe that many public institutions lack accurate and up-to-date land records, creating opportunities for illegal occupation and unauthorised land use. This institutional weakness is further compounded by inadequate monitoring mechanisms, which allow encroachers to exploit poorly defined or unprotected land boundaries.

Similarly, Ugando, Egolum & Sado (2023) note that a significant number of Nigerian universities operate with outdated land tenure records, many of which are still maintained in manual or fragmented formats. These obsolete systems make it difficult for institutions to establish clear ownership claims or respond promptly to land disputes. As a result, universities often find themselves vulnerable to prolonged legal battles, land loss, and strained relationships with host communities. The persistence of these challenges underscores the critical need for improved land documentation and management practices within Nigerian public institutions. In response to these shortcomings, Geographic Information System (GIS) technology has been widely recognised as an effective tool for spatial planning, land demarcation, and boundary management. GIS enables accurate mapping, real-time monitoring, and systematic documentation of land assets, thereby enhancing institutional capacity to detect and prevent encroachment (Balogun, 2019). Despite its proven benefits, the adoption of GIS in Nigerian universities remains limited. Many institutions lack the technical expertise, financial resources, and institutional support required for full-scale implementation. Consequently, the potential of GIS as a proactive land protection tool is yet to be fully realised in the higher education sector.

Although digital technologies have improved the efficiency of land administration, they have also introduced significant cybersecurity risks that threaten the integrity, confidentiality, and availability of land information systems. One of the most common threats is database tampering, where unauthorised users alter or delete digital land records, resulting in fraudulent changes to ownership, boundary information, or land transactions. Such attacks undermine public confidence in land administration and often lead to costly legal disputes. Another emerging challenge is phishing and social engineering attacks targeting land registry personnel. Cybercriminals frequently exploit fraudulent emails, fake login portals, or malicious attachments to obtain administrator credentials, thereby gaining unauthorised access to sensitive land databases. Insider threats also remain a major concern, as privileged users may intentionally manipulate records or abuse administrative privileges for personal gain.

In addition, many conventional land management systems rely on centralised databases that lack robust blockchain-based verification and immutable audit trails, making it difficult to detect unauthorised modifications or establish a trustworthy transaction history. Weak authentication mechanisms, inadequate encryption, ransomware attacks, malware infections, and poor backup and disaster recovery practices further expose digital land records to compromise, data loss, and service disruption (Sikder et al., 2020; Adeyinka, 2024). These vulnerabilities demonstrate that effective land governance increasingly depends not only on sound administrative procedures but also on comprehensive digital security mechanisms that ensure the authenticity, integrity, traceability, and resilience of electronic land records. Consequently, the proposed Digital Security and Land Protection Method seek to address these cybersecurity challenges through secure

authentication, tamper-resistant record management, immutable transaction logging, and blockchain-enabled verification to strengthen trust and transparency in digital land administration.

Beyond physical land management challenges, Nigerian universities also face significant cybersecurity threats arising from increased digitalisation. Akinola et. al (2019) identify poor ICT infrastructure, low levels of cybersecurity awareness, and inconsistent policy enforcement as major contributors to cybersecurity vulnerabilities in Nigerian higher institutions. As universities increasingly rely on digital platforms for academic administration, financial transactions, and data storage, they become attractive targets for cyberattacks such as phishing, ransomware, and unauthorised system access. Cheng and Wang (2022) further argue that although advanced cybersecurity tools, including firewalls, Intrusion Detection Systems (IDS), and encryption protocols, are widely available, their adoption and effective utilisation in Nigerian universities remain minimal. This gap is often attributed to limited funding, inadequate technical expertise, and weak institutional commitment to cybersecurity governance. The consequences of such vulnerabilities extend beyond data breaches, potentially undermining digital land records, surveillance systems, and other technology-driven land protection mechanisms.

Recent studies suggest that integrating geospatial technologies with robust digital security systems offers a promising approach to institutional land protection. Integrated security frameworks that combine GIS-based land monitoring, real-time surveillance, biometric access control, and network security protocols have demonstrated effectiveness in sectors such as urban planning, infrastructure management, and national security (Zikder, Aksu & Uluagac, 2020). These integrated systems enhance situational awareness, enable rapid response to threats, and improve the overall resilience of institutional assets. However, there remains a notable gap in empirical research on the holistic application of such integrated systems within Nigerian universities. Existing studies tend to examine land encroachment or cybersecurity challenges in isolation, without adequately exploring their interconnections. This gap is particularly significant given the increasing digitisation of land management processes and the growing sophistication of both physical and cyber threats facing higher institutions.

Theoretical Discourse

Systems Theory

Systems theory, originally introduced by the biologist Ludwig von Bertalanffy in the 1940s, provides a comprehensive analytical framework for understanding complex phenomena by examining systems as integrated wholes rather than as isolated parts (Checkland, 1981). Over subsequent decades, scholars across disciplines refined the theory, emphasising that the parts of any system are best understood in terms of their relationships with one another and with the wider environment in which the system operates. A core principle of systems theory is that "the parts of a system can best be understood in the context of the relationships with each other and with other systems, rather than in isolation" (Costanza, d'Arge, de Groot, Farber, Grasso, Hannon & van den Belt, 1997). This holistic orientation makes systems theory particularly suitable for analysing digital security and land protection methods in Obafemi Awolowo University (OAU), Ile-Ife, Nigeria, where physical land assets, digital infrastructures, institutional policies, security personnel, and host community dynamics are deeply interconnected.

Obafemi Awolowo University can be conceptualised as a complex socio-technical system comprising multiple subsystems, including land administration, physical security, digital security, governance structures, academic operations, and external community relations. Within this system, land protection is not merely a physical activity involving boundary demarcation or patrols; rather, it is an outcome of continuous interactions among legal frameworks, digital technologies, human actors, institutional norms, and environmental conditions. Systems theory, therefore, provides a robust lens for understanding how digital security tools, such as Geographic Information Systems (GIS), surveillance technologies, land information systems, and

cybersecurity protocols, interact with traditional land management practices to shape land protection outcomes at OAU.

At the core of systems theory is a holistic perspective that views the system as an integrated whole. Applied to OAU, this perspective emphasises that effective land protection cannot be achieved by focusing solely on individual components such as security personnel, physical fences, or isolated digital tools. Instead, land protection must be understood as the emergent outcome of coordinated interactions among physical infrastructure, digital security systems, institutional policies, administrative capacity, and community engagement. For instance, the deployment of GIS-based land mapping without adequate institutional policies or trained personnel may yield limited benefits. Similarly, strong cybersecurity infrastructure without accurate geospatial documentation of university land boundaries may fail to prevent encroachment. Systems Theory highlights that these components must function together as a unified system (Jackson, 2003). Adopting a holistic approach, OAU can align its digital security initiatives with land administration processes, legal frameworks, and physical surveillance mechanisms, thereby improving overall land protection effectiveness. This holistic orientation is particularly relevant in the context of increasing land encroachment, illegal mining, and unauthorised land use around OAU (De Lucia, 2020). Such challenges are not purely security issues; they are also influenced by urbanisation pressures, socio-economic dynamics of host communities, institutional weaknesses, and technological gaps. Systems Theory allows these diverse factors to be analysed collectively, providing a more comprehensive understanding of the land protection problem.

A fundamental principle of Systems Theory is interconnectedness, the idea that components of a system are interdependent, and changes in one part can significantly affect others. In the context of digital security and land protection at OAU, this principle underscores the strong linkages between digital systems, physical security arrangements, administrative decision-making, and external community relations (Michailakis & Schirmer, 2014). For example, weaknesses in digital land records or the absence of up-to-date GIS data can undermine physical security efforts by making it difficult to accurately identify encroached areas. Similarly, poor coordination between the university's ICT unit and its security department may lead to fragmented responses to land threats. Systems Theory emphasises that these interdependencies must be recognised and managed deliberately. Enhancing one subsystem, such as introducing surveillance drones or digital boundary mapping, requires corresponding adjustments in policy enforcement, staff training, and data governance to ensure system-wide effectiveness. In addition, land protection at OAU is interconnected with broader socio-economic and environmental systems. University land use decisions affect surrounding communities, ecological sustainability, and town-gown relations. Conversely, external pressures such as urban expansion and community land claims directly influence the university's internal land protection strategies. Systems Theory helps to illuminate these bidirectional relationships, encouraging land protection approaches that are sensitive to both internal institutional needs and external environmental and social dynamics.

Feedback loops, both positive and negative, are central to understanding system behaviour within Systems Theory. Feedback loops occur when a system's output influences its future behaviour, either by reinforcing existing patterns (positive feedback) or by stabilising and correcting deviations (negative feedback). In the context of OAU, feedback mechanisms play a critical role in shaping land protection outcomes. Positive feedback loops may arise when successful land encroachment leads to further encroachments. For example, if illegal occupation of university land goes undetected due to weak digital surveillance or poor land documentation, it may embolden other actors to engage in similar activities, thereby escalating land loss. Conversely, negative feedback loops can stabilise the system when effective digital monitoring detects encroachment early, prompting swift enforcement actions that deter further violations. Systems theory encourages identifying and managing these feedback loops. By integrating real-time surveillance, GIS monitoring, and digital reporting systems, OAU can create negative feedback mechanisms that quickly respond to threats, correct deviations, and restore system balance. Understanding feedback dynamics also enables the university to anticipate unintended consequences of interventions, for instance, how increased surveillance might affect community perceptions or require complementary communication strategies to maintain positive town-gown relations.

Another key concept in Systems theory is emergent behaviour, the idea that complex system-level outcomes arise from interactions among components and cannot be fully understood by examining individual parts in isolation (Food and Agriculture Organisation, n.d). In land protection at OAU, emergent behaviours may include patterns of encroachment, shifts in community attitudes, or changes in institutional capacity that result from the combined effects of digital security tools, policy decisions, and enforcement practices. For example, the introduction of an integrated digital land management system may not only improve boundary monitoring but also enhance institutional transparency, data-driven decision-making, and stakeholder confidence. Conversely, poorly coordinated digital security initiatives may unintentionally create loopholes, increase administrative burdens, or generate resistance from staff or host communities. Systems Theory helps researchers and policymakers recognise these emergent outcomes, enabling more adaptive and responsive land protection strategies (Goldstein, 1999). Focusing on emergent behaviour, the theory also underscores the importance of continuous system evaluation. Digital security and land protection methods at OAU should not be viewed as static solutions but as evolving processes that require regular assessment and adjustment in response to changing environmental, technological, and social conditions.

Systems theory posits that systems are open, meaning they continuously exchange information, energy, and resources with their environment. Obafemi Awolowo University operates as an open system, interacting with government agencies, host communities, security institutions, and technological environments (Heylighen, 1992). Digital security systems rely on information exchange, data collection, processing, storage, and dissemination to function effectively. In land protection, information exchange includes geospatial data sharing, incident reporting, policy communication, and coordination between physical and digital security units. External factors such as technological advancements, cybersecurity threats, and urban development trends also influence internal system dynamics (Hitchins, 2003). Systems Theory emphasises that effective land protection at OAU must account for these external influences by adopting flexible, adaptive digital security frameworks. Understanding information exchange also highlights the importance of cybersecurity. As land records, maps, and surveillance data become digitised, protecting these information assets from cyber threats becomes integral to land protection. A breach in digital systems can compromise land records, undermine legal claims, and weaken institutional authority. Systems Theory thus supports integrating cybersecurity protocols into land protection strategies, ensuring that information flows remain secure and reliable (Holling, 2001). Applying Systems Theory to digital security and land protection at Obafemi Awolowo University underscores the need for an integrated, multidisciplinary approach. Rather than relying on fragmented or reactive measures, the university must develop a coherent system that aligns digital technologies, physical security, institutional policies, and stakeholder engagement. GIS-based land mapping, surveillance systems, and cybersecurity tools should function as interconnected components within a unified land protection framework.

Methodology

The study uses a survey research design, which facilitates the systematic collection of data from relevant stakeholders (Registry, Security Department, and Legal Unit) involved in land administration, digital security management, and land protection practices. The survey research design enables the researcher to capture patterns, trends, and variations in responses while also allowing for comparative analysis across different categories of respondents. Primary data and secondary data (Review of institutional documents, including land policies, digital security protocols, GIS maps, and historical encroachment records) were employed for the study. Primary data were generated through semi-structured interviews, which provided flexibility for respondents to express their experiences, perceptions, and expert opinions on digital security and land protection methods, while structured questionnaires were used to obtain standardised quantitative data suitable for statistical analysis. In addition, secondary data were sourced through a systematic review of relevant institutional documents, including land policies, security department records, GIS maps, and historical encroachment records, to provide contextual background, validate primary data findings, and establish trends over time.

Purposive sampling and stratified random sampling techniques were used to determine the sample size of 20 Respondents. Purposive sampling enabled the selection of key informants with specialised knowledge and direct involvement in digital land security and protection processes, while stratified random sampling was used to ensure adequate representation of different stakeholder groups, institutions, and geographical or administrative strata relevant to the study. This combination of sampling techniques enhances representativeness while also ensuring that critical perspectives are adequately captured. Data were analysed using content analysis. Qualitative data from interviews were transcribed, coded, and organised into themes that reflect recurring patterns and emerging issues related to digital security and land protection methods. The integration of both analytical approaches allowed for triangulation of findings and deeper interpretation of results.

Ethical Consideration

This study did not involve human participants, animals, clinical procedures, or the collection of primary personal data. The research was based entirely on the review and synthesis of published literature, policy documents, and publicly available technical and institutional information to develop the proposed Digital Security and Land Protection Method. Consequently, formal ethical approval and informed consent were not required. Notwithstanding, the study adhered to the highest standards of research ethics and academic integrity. All sources of information were accurately acknowledged and cited to ensure proper attribution of intellectual property and to avoid plagiarism. In developing the proposed framework, particular attention was paid to the ethical implications of digital land governance, including the principles of data privacy, confidentiality, cybersecurity, transparency, accountability, and responsible management of digital land records. The proposed method is intended to enhance the security and integrity of land administration systems while respecting applicable legal, institutional, and ethical standards governing digital information and property rights.

Current State of Digital Security Infrastructure in Obafemi Awolowo University (OAU)

The digital security infrastructure of Obafemi Awolowo University (OAU) remains partially developed and largely supplementary to traditional land administration practices. OAU's land security architecture is anchored in traditional land protection instruments (Makinde, Ridwan & Saragih, 2021), including approved layout plans, survey and cadastral drawings, physical boundary beacons, routine site inspections, and historical land documentation. Approved layout plans provide the formal spatial structure for land use across the campus, while survey drawings legally define boundaries and the extent of ownership. Physical beacons serve as on-ground boundary indicators, complemented by periodic inspections aimed at identifying encroachments. Historical land records and archival documents further reinforce institutional claims and support dispute resolution. These mechanisms remain central to land protection but are inherently static and depend heavily on human intervention.

Digital security infrastructure at OAU is currently most visible through the application of Geographic Information System (GIS) technologies[1], which have been used to generate spatial data and campus maps and to analyse patterns of human activity and security incidents (Makinde, Ridwan, & Saragih, 2021). Although GIS deployment has been primarily oriented towards crime analysis, its underlying spatial capabilities are directly relevant to land protection, particularly in monitoring land-use intensity, access routes, and areas of vulnerability (Oludare & Eyinade, 2025). However, these digital tools have not been fully institutionalised within land administration processes. Crucially, traditional land protection instruments at OAU are not systematically digitised or integrated into a central spatial database. Approved layout plans, survey drawings, and beacon coordinates are rarely converted into georeferenced digital formats that can support automated monitoring or spatial verification. As a result, the digital infrastructure functions mainly as a support tool rather than as an operational system for real-time detection of encroachment or unauthorised land-use changes.

OAU currently lacks advanced digital monitoring mechanisms such as satellite-based change detection, drone surveillance, geo-fencing technologies, or real-time alert systems that could enhance boundary enforcement. The absence of these tools limits the University's capacity to detect gradual encroachments, especially in peripheral or low-activity zones of the campus[2]. Consequently, land protection remains largely reactive, with interventions typically occurring after encroachments become physically evident. The current state of digital security infrastructure in OAU reflects a hybrid but weakly integrated system, where traditional land protection methods dominate, and digital tools play a limited, non-systematic role. While GIS applications demonstrate the University's potential to adopt spatially driven land security solutions, the lack of integration between digital technologies and established land records constrains effective encroachment control. Strengthening digital security for land protection will therefore require the deliberate digitisation of land documents, integration of physical boundary data into GIS platforms, and adoption of monitoring technologies capable of supporting proactive land governance.

Analysis of the University's Land Tenure System and Current Protection Mechanisms

Obafemi Awolowo University operates under a statutory land tenure arrangement, deriving its landholding authority from federal government ownership and allocation. As a federally owned institution, OAU possesses extensive land assets (a total landed area of 5,609 hectares) designated for academic, residential, agricultural, and infrastructural purposes[3]. However, the openness of the campus and its vast territorial extent present persistent challenges to land protection and boundary enforcement. The University's land tenure system is characterised by institutional ownership with administrative control, but practical protection mechanisms remain weak due to limited digitisation of land records and boundary data. Although spatial data exists in the form of satellite imagery and GIS-generated campus maps, these resources are primarily utilised for academic research and crime analysis rather than comprehensive land governance and encroachment prevention (Oludare & Eyinade, 2025).

Current land protection mechanisms at OAU rely heavily on physical surveillance, manual patrols, and traditional security presence, particularly around sensitive zones. These mechanisms are constrained by manpower limitations and lack the technological sophistication required to monitor land use changes, detect encroachments, or secure peripheral boundaries effectively. The GIS crime hotspot analysis indirectly reveals this weakness, as several identified hotspots—such as halls of residence and commercial nodes are in areas with high accessibility and weak environmental controls (Oludare & Eyinade, 2025). Importantly, the absence of a fully integrated digital land information system (DLIS) undermines the University's capacity to protect its land assets. Digital cadastral mapping, geo-fencing, and automated alert systems—which could link land boundaries to security infrastructure—are either underdeveloped or entirely absent. This gap exposes university land to risks such as informal encroachment, unauthorised commercial activities, and security breaches, particularly at the campus peripheries.

The finding further demonstrates that security vulnerabilities are spatially concentrated and predictable, reinforcing the relevance of environmental criminology theories such as Routine Activity Theory and Crime Pattern Theory (Oludare & Eyinade, 2025). Applied to land tenure, these theories suggest that poorly monitored land spaces, especially those lacking capable digital guardianship, are more susceptible to illegal occupation and criminal activity. The identification of "cool spots" such as the Maintenance area (characterised by restricted access and controlled activity) illustrates how structured land use and consistent oversight can reduce vulnerability (Oludare & Eyinade, 2025).

Assessment of Digital Security Technologies and Institutional Coordination for Land Protection at Obafemi Awolowo University, Ile-Ife

This study also evaluated the effectiveness of existing digital security technologies in addressing land protection challenges in Obafemi Awolowo University (OAU), Ile-Ife. The focus is on determining how far technologies such as Geographic Information Systems (GIS), digital surveillance tools, and cybersecurity

mechanisms contribute to preventing land encroachment and strengthening institutional land governance. In an interactive session with one of the ICT staff on the subject matter, the following question was asked: What digital security technologies are currently deployed in OAU for land protection purposes? ICT staff responded that:

> At present, digital security technologies specifically designed for land protection are limited in OAU. We have general ICT infrastructure such as network systems, servers, and basic databases, but these are not purposefully structured for land protection. Some land-related documents are stored digitally, and there are a few GIS files within the Physical Planning Unit, but there is no centralised digital land security system. Surveillance technologies like CCTV are available, but they are mainly deployed within campus buildings rather than land boundary areas[4].

The Chief Security Officers disclosed that Digital security technologies available to us are limited and not specifically designed for land protection. CCTV cameras exist within the core campus areas, but there are few or no digital surveillance tools covering land boundaries. Communication is mainly through radios and mobile phones, and we do not have access to real-time digital land monitoring systems. Another ICT staff member further noted that GIS and digital databases have the potential to be very effective, but in practice, their effectiveness is currently low. Land boundary information is not fully digitised, and where digital records exist, they are often outdated or incomplete. GIS is not routinely used to monitor land boundaries or detect encroachment. As a result, digital databases do not yet provide a reliable or comprehensive platform for managing the University's land boundaries.

Furthermore, to know the extent to which digital tools such as GIS are used in land boundary mapping and monitoring, one of the planning physical units stated that:

> GIS tools are used to a very limited extent, mainly for internal planning and development layout purposes. Comprehensive GIS-based land boundary mapping has not been fully implemented. Where GIS data exists, it is often incomplete or outdated, and it is not routinely used for monitoring land boundaries or detecting encroachment. The absence of a centralised GIS system makes digital monitoring difficult[5].

Concerning the methods that are currently used to manage and protect the University's land, a participant in the Physical Planning Unit disclosed

> Our unit primarily relies on traditional land administration methods such as approved layout plans, survey drawings, physical beacons, site inspections, and historical land documents. Most of these records are maintained in hard-copy format, although some documents have been scanned for internal reference. Land protection is largely reactive and depends on periodic inspections and reports from security personnel or staff members[6].

It was further discovered that there are existing land documentation systems which are moderately effective but have significant limitations. While traditional survey plans and layout documents provide historical evidence of land ownership, their effectiveness is reduced by poor digitisation and limited accessibility. During land disputes, retrieving and validating these documents can be time-consuming, and the lack of digitally authenticated records weakens enforcement and legal processes.

To assess the effectiveness of the digital security technology, it was asked what cybersecurity measures are in place to protect digital land records. One of the ICT staff added that:

> "General cybersecurity measures such as password controls, access restrictions, and network firewalls are in place across the University's ICT systems. However, there are no specialised

> cybersecurity protocols dedicated specifically to protecting digital land records or GIS data. Access to land-related digital information is not always role-based, and encryption is not consistently applied. This exposes sensitive land data to risks such as unauthorised access or accidental data loss[7]."

Further evaluation found that the Security Unit currently plays a certain role in protecting the University's land. According to the Chief Security Officer, the Security Unit is primarily responsible for physical patrols, monitoring suspicious activities, and responding to reports of land encroachment. They patrol designated areas, especially at the outskirts of the campus, and work with community leaders and other units when encroachment issues arise. Most of the operations are manual and depend on human observation and intelligence gathering. In relation to the use of surveillance systems in detecting land encroachment, it was disclosed by one of the security staff that:

> Existing surveillance systems are largely ineffective in detecting land encroachment. Most encroachment cases are discovered during routine patrols or after receiving reports from staff or nearby communities. Since surveillance cameras are not installed around boundary areas, they do not contribute meaningfully to early detection or prevention of encroachment[8].

Despite several efforts by these units, technical challenges affect the effectiveness of digital security systems in OAU. One of the ICT staff posited that several technical challenges affect the effectiveness of digital security. These include unstable power supply, outdated hardware, limited system upgrades, and insufficient funding for maintenance. In addition, there is a shortage of specialised technical skills required to manage advanced GIS and surveillance systems. These challenges often lead to system downtime and discourage the consistent use of digital technologies for land protection. This was complemented by one of the physical planning units that:

> The major challenges include inadequate funding, limited access to modern GIS software, lack of specialised technical training, and poor integration with ICT systems. In addition, many land records predate digital documentation and require extensive effort to digitise. Institutional delays and bureaucratic procedures also affect the timely adoption of digital tools[9].

On the part of the security operatives, the key challenges include lack of equipment, limited technical training, and absence of digital monitoring tools for boundary areas. One of the officers buttresses that they also face manpower constraints and logistical challenges, especially when patrolling large land areas. Without access to digital land maps or real-time monitoring systems, their response is often delayed and reactive.

During effectiveness evaluation, it was observed that there is collaboration among these three units. This was highlighted by one of the ICT staff and one of the Physical Planning Unit staff: collaboration exists, but it is largely informal and reactive. The ICT unit typically provides technical support when requested, rather than being actively involved in land protection planning. There is no structured platform for regular data sharing or joint decision-making between ICT, Physical Planning, and Security units. This limits the effectiveness of digital tools and reduces institutional coordination on land protection matters. This claim was largely supported by the security unit that:

> Collaboration exists but is mostly informal. We usually work with the Physical Planning Unit during site inspections and enforcement actions, and we contact the ICT Unit when technical support is required. However, there is no centralised system that links security operations with digital land data or surveillance information, which limits coordinated action[10].

With this collaboration, each unit was asked to assess the effectiveness of digital security technologies in preventing land encroachment. The ICT unit found that, at the moment, existing digital security technologies

are not very effective in preventing land encroachment. Most encroachment cases are detected through physical patrols or reports from community members rather than through digital monitoring systems. The lack of integrated GIS mapping and boundary surveillance means that digital technologies play a minimal role in early detection or prevention. This was further buttressed by one of the ICT staff who said:

> Current digital security technologies are not effective in preventing land encroachment. Prevention mainly depends on physical presence and community intelligence. Without digital tools such as boundary surveillance, GIS maps, or early warning systems, it is difficult to prevent encroachment before it escalates[11].

Beyond technological availability, the effectiveness of digital security technologies at OAU is significantly shaped by the level of institutional coordination among relevant units. Effective land protection requires seamless collaboration between the ICT unit, physical planning department, land management office, and security services. Where digital tools operate in silos, critical information sharing is delayed or lost, weakening institutional response to encroachment threats. Empirical evidence from Nigerian universities suggests that fragmented governance structures often undermine the operational benefits of digital security systems, even where the technologies themselves are functional.

Human capacity remains a decisive factor in determining the effectiveness of digital security technologies for land protection. Technologies such as GIS platforms and surveillance systems require skilled personnel for data interpretation, system maintenance, and operational decision-making. At OAU, variations in technical expertise among staff may affect how effectively digital tools are utilised. Through interviews and questionnaire responses, this study assesses staff competency, training exposure, and institutional support for digital security operations. Limited technical capacity is expected to correlate with underutilization of available technologies, thereby reducing their effectiveness in mitigating land encroachment. The sustainability and reliability of digital security technologies are critical determinants of their effectiveness in land protection. Factors such as power supply instability, inadequate funding for system maintenance, and reliance on obsolete hardware often constrain digital security operations in Nigerian public institutions. In OAU, frequent system downtime or inconsistent updates are likely to weaken land monitoring efforts and reduce institutional confidence in digital security solutions.

The effectiveness of digital security technologies also has legal and enforcement implications for land protection at OAU. Digitally documented land boundaries, surveillance records, and secure data archives provide verifiable evidence that can support legal action against encroachers. This study found that where digital systems fail to produce credible and accessible records, enforcement efforts may be weakened, regardless of technological investment. Strengthening the penitentiary value of digital security outputs therefore constitutes a critical dimension of effectiveness.

Innovative and Technology-Driven Strategies for Sustainable Land Security at Obafemi Awolowo University

This study examined innovative and technology-based solutions capable of improving land security in Obafemi Awolowo University, with a focus on developing sustainable, scalable, and institutionally appropriate interventions. The objective moves beyond evaluating existing systems to proposing forward-looking solutions grounded in empirical evidence and institutional realities. In an interactive session with one of the ICT staff on the subject matter, the question was asked: What innovative digital solutions would you recommend to improve land security in OAU? This question was met with a response from one of the ICT staff.

> I would recommend developing an integrated digital land management system that combines GIS mapping, digital land registries, surveillance data, and cybersecurity controls. Drone-based surveillance would also be very useful for monitoring large and remote land areas. In

> addition, implementing role-based access control and encrypted storage for land records would significantly improve data security[12].

This proposition relates to the position of one of the physical planning units that, from a planning perspective, the most effective solution would be the establishment of a centralised digital land registry supported by a comprehensive GIS platform. This would clearly define land boundaries, improve documentation, and support enforcement. Drone technology would also be useful for aerial surveys and boundary monitoring, especially in remote or large land areas. A close remark to this is the suggestion of the security unit, where one of the unit's members added that:

> Drone surveillance would greatly improve land security by allowing us to monitor large areas quickly and safely. Installing surveillance cameras at strategic boundary points would also help. In addition, access to digital land maps and GIS systems would improve our understanding of boundary limits and support enforcement activities[13].

From this common position, it was further pressed how feasible the adoption of an integrated digital land management system is in the University. The ICT unit and the physical planning unit were in the same position that the adoption of an integrated digital land management system is feasible, but it would require strong institutional commitment. The main challenges would be funding, staff training, and policy support. With phased implementation and support from external funding bodies such as TETFund, the system can be successfully deployed and sustained. This position was further hammered by one of the security officers who added that:

> Technology-based land security solutions are feasible if supported by proper training, funding, and institutional policies. Security officers are willing to adopt new technologies, but this requires management support, clear operational guidelines, and sustained equipment maintenance[14].

Based on this, the study posited that sustaining innovative land security solutions would require regular training in GIS, cybersecurity, and digital surveillance technologies. ICT staff would need advanced technical training, while Physical Planning and Security personnel would require basic digital literacy and system usage training. Capacity building should be continuous and supported by institutional policies and incentives. This was strongly supported by one of the staff in the physical planning unit.

> Planning staff would also benefit from exposure to modern land administration practices and digital tools. Capacity building should be institutionalised rather than treated as a one-off activity[15].

Coupled with this claim, this study suggested that security officers need training in the use of surveillance technologies, basic GIS interpretation, and digital reporting systems. Continuous training is important to ensure that officers can effectively use new tools and adapt to evolving security challenges. Capacity building should be part of routine security development programs.

Theoretically, the examination of innovation is anchored in socio-technical systems theory, which underscores the need to align technological advancement with organisational capacity and social context. For OAU, innovative land security solutions must not only be technologically sophisticated but also compatible with administrative structures, budgetary constraints, and stakeholder relations, particularly with host communities. On the other hand, empirical insights derived from interviews and institutional document reviews inform the identification of viable technology-based solutions. One key innovation examined is the establishment of an integrated digital land management system that combines GIS mapping, digital land registries, surveillance technologies, and cybersecurity protocols into a single operational framework. Such

integration is expected to improve coordination between the ICT unit, physical planning department, and security services, thereby reducing fragmentation in land governance.

The study further found that innovative solutions for improving land security at OAU must extend beyond hardware and software deployment to include policy and governance reforms. Digital land security initiatives require clear institutional policies that define roles, responsibilities, and accountability mechanisms across administrative units. Thus, embedding innovation within formal policy frameworks enhances sustainability and reduces the risk of technology abandonment. Similarly, technology-based land security solutions are more effective when complemented by structured engagement with host communities. In the OAU, community resistance and informal land claims often complicate enforcement efforts. Innovative approaches such as publicly accessible digital boundary maps and community sensitisation using geospatial visualisations can enhance transparency and reduce conflict.

Nevertheless, the study posited that the long-term success of innovative land security solutions depends on financial and operational sustainability. Technologies such as drones, integrated GIS platforms, and advanced cybersecurity systems require sustained funding for maintenance, upgrades, and capacity development. Therefore, solutions that align with the University's financial capacity and administrative structure are more likely to be adopted and sustained. Conclusively, an important dimension of innovation examined in this study is the replicability of proposed land security solutions across Nigerian universities. OAU serves as a case study through which broader institutional learning can be derived.

Discussion of Findings

The study further examined the effectiveness of digital security technologies on land protection and explored innovative, technology-based solutions for improving land security in Obafemi Awolowo University (OAU), Ile-Ife. Drawing on triangulated data from ICT staff, Physical Planning Unit personnel, and Security Officers, the discussion provides an interpretive analysis of how institutional, technological, and human factors interact to shape land security outcomes within the University. A central finding of the study is that digital security technologies in OAU currently exhibit limited effectiveness in addressing land encroachment challenges. Although basic digital infrastructure exists, its application to land protection remains fragmented and peripheral. This finding aligns with earlier studies on Nigerian public institutions, which observe that digital tools are often adopted in isolation without being integrated into core governance and enforcement processes (Akinola et al, 2019; Cheng & Wang, 2022). The present study extends this literature by demonstrating that the issue is not merely technological inadequacy, but rather a systemic disconnect between digital systems and institutional land governance practices.

The underutilization of Geographic Information Systems (GIS) emerged as a critical constraint on land protection effectiveness. While GIS has been widely recognised as a powerful tool for land demarcation, monitoring, and dispute resolution (Adeyinka, 2024), findings from OAU reveal that GIS usage is largely confined to limited planning functions rather than active land protection. The absence of a centralised, continuously updated GIS-based land registry undermines the University's capacity to assert spatial authority over its land. This situation reinforces the argument that digital land management systems must be institutionalised rather than treated as optional technical add-ons. Digital surveillance technologies were also found to have minimal impact on land protection, particularly at land boundary areas where encroachment is most prevalent. The concentration of surveillance infrastructure within academic and residential zones reflects a misalignment between security priorities and land protection needs. Similar patterns have been reported in studies of campus security in developing contexts, where surveillance technologies are deployed primarily for internal security rather than territorial protection (Zikder, Aksu & Uluagac, 2020). The implication is that surveillance effectiveness depends not only on technology availability but also on strategic deployment guided by land-specific risk assessments.

Cybersecurity weaknesses further compound the limitations of digital land protection at OAU. Findings indicate that digital land records and spatial data are not protected by specialised cybersecurity protocols, increasing the risk of unauthorised access, data manipulation, or loss. This undermines the credibility of digital records for enforcement and legal purposes. In line with Cheng and Wang (2022), the study demonstrates that weak cybersecurity governance erodes trust in digital systems and discourages their use in sensitive domains such as land administration. Furthermore, interdepartmental fragmentation emerged as a major institutional barrier. The lack of systematic data sharing between ICT, Physical Planning, and Security units prevents the effective use of available digital tools. This finding strongly supports the core proposition of socio-technical systems theory, which emphasises that technological effectiveness is contingent upon alignment with organisational structures and social processes. In the absence of coordination mechanisms, digital technologies fail to achieve their intended impact regardless of their technical sophistication.

Regarding innovative and technology-based solutions, the study reveals strong institutional consensus on the need for integrated digital land security frameworks. Stakeholders across all units identified integrated GIS platforms, centralised digital land registries, and coordinated surveillance systems as viable solutions. This aligns with global best practices in smart campus and digital land governance initiatives, which emphasise integration, interoperability, and centralised data management (Zikder, Aksu & Uluagac, 2020). The study's contribution lies in contextualising these innovations within the operational realities of a Nigerian federal university.

It was also found that the strong support for drone-based surveillance reflects a pragmatic response to the spatial challenges posed by OAU's extensive landmass. Drones offer real-time monitoring capabilities, rapid coverage of inaccessible areas, and visual evidence for enforcement. The enthusiasm expressed by security and planning personnel suggests operational readiness for such innovation, provided issues of training, regulation, and funding are addressed. This finding reinforces the argument that innovation adoption is driven as much by perceived utility as by technological availability.

Capacity building emerged as a cross-cutting requirement for both effectiveness and innovation. The study confirms that human capital constraints significantly limit the deployment and sustainability of digital security technologies. This supports socio-technical theory's assertion that human actors are central to system performance. Without targeted training, digital literacy, and institutional incentives, even well-designed technologies are likely to remain underutilised. Another decisive factor identified was funding sustainability and policy support. Respondents acknowledged the cost implications of innovative technologies, but they expressed optimism about phased implementation and external funding support. This finding aligns with studies on digital transformation in public institutions, which highlight the importance of aligning technological ambition with financial and administrative capacity (Ugando, Egolum & Sado, 2023).

Although this study focuses on Obafemi Awolowo University (OAU), the challenges associated with securing digital land records are not unique to Nigeria. Universities worldwide increasingly rely on digital land information systems to manage institutional assets, making them vulnerable to cybersecurity threats such as unauthorised database modification, ransomware attacks, phishing, insider threats, and weak access controls (Von Solms & Van Niekerk, 2021; ENISA, 2023). A comparison with the University of Cape Town (UCT), South Africa, illustrates both shared challenges and important institutional differences. Like OAU, UCT manages extensive land and infrastructure assets that require secure digital record management. However, UCT operates within a more mature digital governance environment supported by South Africa's Protection of Personal Information Act (POPIA), institutional information governance frameworks, and established cybersecurity policies that strengthen data protection and access management (Republic of South Africa, 2013; Information Regulator South Africa, 2023). These institutional arrangements contribute to stronger protection of digital assets through formal information governance, risk management, and cybersecurity compliance.

By contrast, OAU continues to face challenges associated with fragmented land records, limited cybersecurity infrastructure, reliance on conventional database management systems, and the absence of immutable verification mechanisms for land transactions. These conditions increase the risk of database tampering, unauthorised alterations, insider misuse, and fraudulent land documentation (Balogun, 2019; Adeyinka, 2024). While universities in both countries face evolving cyber threats, the comparison suggests that robust governance frameworks, comprehensive cybersecurity policies, and emerging technologies such as blockchain-based verification can significantly enhance the integrity and security of digital land administration. Consequently, the proposed digital security and land protection method is designed not only to address OAU's specific challenges but also to provide a scalable and adaptable framework that can be implemented by universities and higher education institutions seeking to strengthen the security, transparency, and accountability of digital land management systems. Based on the foregoing, the discussion demonstrates that land security challenges in OAU are not simply the result of inadequate technology, but rather the outcome of systemic socio-technical misalignment. Digital security technologies, when fragmented and weakly governed, cannot effectively protect institutional land. However, when embedded within integrated frameworks supported by policy reform, capacity building, and interdepartmental collaboration, these technologies hold significant potential to transform land protection practices.

Conclusion

This study set out to investigate digital security and land protection methods in Obafemi Awolowo University (OAU), Ile-Ife, with the overarching aim of proposing an integrated framework for improved institutional land security. In addressing the first objective, the study examined the current state of digital security infrastructure in OAU and found that while digital tools exist, their deployment remains limited and uneven across administrative units. The findings reveal gaps in infrastructure availability, system integration, and cybersecurity preparedness, underscoring the need for coordinated digital security planning to support effective land protection. In line with the second objective, the study analysed the University's land tenure system and existing land protection mechanisms. The analysis indicates that OAU's land governance framework relies heavily on traditional documentation and physical monitoring, which are increasingly inadequate in the face of rising urbanisation pressures and sophisticated encroachment activities. Incomplete land records, weak enforcement structures, and limited use of geospatial documentation were identified as key factors contributing to institutional vulnerability. These challenges highlight the urgency of modernising land tenure management through digital documentation and spatial technologies.

Addressing the third objective, the study evaluated the effectiveness of digital security technologies in enhancing land protection at OAU. The findings suggest that technologies such as Geographic Information Systems (GIS), digital surveillance tools, and cybersecurity mechanisms possess significant potential to improve land monitoring, documentation, and enforcement. However, their effectiveness is currently constrained by fragmented implementation, limited technical capacity, infrastructural challenges, and weak interdepartmental coordination. The study demonstrates that without institutional integration and sustained operational support, digital security technologies cannot achieve optimal impact. In response to the fourth objective, the study examined innovative and technology-based solutions capable of improving land security in OAU. The analysis identified integrated digital land management systems, drone-based surveillance, and strengthened cybersecurity governance as viable and context-appropriate solutions. These innovations, when combined with policy reforms, capacity building, and stakeholder engagement, offer practical pathways for addressing land encroachment and strengthening institutional land governance. The study emphasises that innovation must be both technologically sound and institutionally sustainable.

Anchored in socio-technical systems theory, the study underscores the interdependence between technology, institutional structures, and human actors in achieving effective land protection. Digital security tools must be embedded within organisational processes, supported by skilled personnel, and reinforced by clear policies and enforcement mechanisms. This theoretical perspective provides a holistic understanding of why technological solutions alone are insufficient without corresponding institutional reforms.

In conclusion, this study provides a comprehensive and policy-relevant framework for strengthening digital security and land protection in Obafemi Awolowo University, Ile-Ife. With a systematic address of the objectives researched, the study offers actionable insights for university administrators, policymakers, and security managers. The proposed integrated approach not only enhances land security at OAU but also serves as a replicable model for other Nigerian universities facing similar land encroachment challenges.

Funding Statement

This research was funded by the 2024-2025 merged TETFund Intervention in Research Project (RP) IBR (BATCH 15)

Endnotes

[1] Interview with a Deputy-Director at the Registry Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[2] Interview with a Record Officer at the PPDU Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[3] Interview with a Liaison Officer at the Legal Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[4] Interview with an ICT Staff at the Registry, Computer Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[5] Interview with a Liaison Officer at the Physical Planning Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[6] Interview with a Participant at the Physical Planning Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[7] Interview with an ICT Staff at the Physical Planning Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[8] Interview with a Chief Security Officer at the Security Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[9] Interview with a Liaison Officer at the Physical Planning Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[10] Interview with a Chief Security Officer at the Security Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[11] Interview with an ICT Staff at the Registry, Computer Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[12] Interview with an ICT Staff at the Physical Planning Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[13] Interview with a Chief Security Officer at the Security Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[14] Interviews with a cross-section of Security Officers at the Security Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

[15] Interviews with a Deputy-Director at the Physical Planning Unit of Obafemi Awolowo University, Ile-Ife, Nigeria

References

Adeyinka, R. B. (2024). Smart land governance for sustainable development in Nigeria. *African Journal on Land Policy and Geospatial Sciences, 7*(1), 348–365. https://doi.org/10.48346/IMIST.PRSM/ajlp-gs.v7i1.46087

Akinola et al. (2019). *Quantitative evaluation of cyber-attacks on a hypothetical school computer network*. Journal of Information Security, 10(3),Akino 103–116. DOI: 10.4236/jis.2019.103006

Angelsen, A. (2010). Policies for reduced deforestation and their impact on agricultural production. *Proceedings of the National Academy of Sciences of the United States of America,* **107**(46), 19639–19644. https://doi.org/10.1073/pnas.0912014107

Balogun, T. F. (2019). Development and implementation of GIS-based property tax management system for Benin City, Nigeria. *African Journal on Land Policy and Geospatial Sciences, 2*(3), 97–112. https://doi.org/10.22004/ag.econ.334222

Brauman, K. A., Daily, G. C., Duarte, T. K., & Mooney, H. A. (2007). The nature and value of ecosystem services: An overview highlighting hydrologic services. *Annual Review of Environment and Resources, 3*2, 67–98

Checkland, P. (1981). *Systems thinking, systems practice*. Chichester: John Wiley & Sons.

Cheng, E. C. K., & Wang, T. (2022). *Institutional strategies for cybersecurity in higher education institutions*. *Information, 13*(4), 192. https://doi.org/10.3390/info13040192

Costanza, R., d'Arge, R., de Groot, R., Farber, S., Grasso, M., Hannon, B., Limburg, K., Naeem, S., O'Neill, R. V., Paruelo, J., Raskin, R. G., Sutton, P., & van den Belt, M. (1997). *The value of the world's ecosystem services and natural capital. Nature, 387*(6630), 253–260. https://doi.org/10.1038/387253a0

Daily, G. C. (1997). *Nature's services: Societal dependence on natural ecosystems*. Washington DC: Island Press

Davenport, C. (2017, December 4). Trump drastically reduces size of Bears Ears and Grand Staircase monuments in Utah. *The New York Times*. https://www.nytimes.com/2017/12/04/climate/trump-bears-ears.html

De Lucia, V. (2020). *The ecosystem approach: A holistic perspective to marine biodiversity conservation*. International Institute for Environment and Development. https://www.iied.org/ecosystem-approach-holistic-perspective-marine-biodiversity-conservation

Dixon, J. A., & Sherman, P. B. (1990). *Economics of protected areas: A new look at benefits and costs*. Washington DC: Island Press

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape 2023*. Publications Office of the European Union. https://doi.org/10.2824/782573

Food and Agriculture Organization of the United Nations. (n.d.). *Integrated landscape management*. FAO Land & Water Division. https://www.fao.org/land-water/overview/integrated-landscape-management/en/

Goldstein, J. (1999). *Emergence as a construct: History and issues. Emergence: Complexity and Organization, 1*(1), 49–72. https://doi.org/10.1207/s15327000em0101_4

Heylighen, F. (1992). Principles of systems and cybernetics. In G. de Zeeuw, M. V. Ulrich, & R. Flood (Eds.), *Cybernetics and systems: Proceedings of the 10th European meeting on cybernetics and systems research* (pp. 3–31). World Scientific.

Hitchins, D. (2003). *Systems Engineering: A 21st century systems methodology*. John Wiley & Sons.

Holling, C. S. (2001). Understanding the complexity of economic, ecological, and social systems. *Ecosystems, 4*(5), 390–405. https://doi.org/10.1007/s10021-001-0101-5

Information Regulator South Africa. (2023). *Guidance notes on the Protection of Personal Information Act (POPIA)*. https://inforegulator.org.za/guidance-notes/

Jackson, M. C. (2003). *Systems thinking: Creative holism for managers*. John Wiley & Sons.

Kumar, P. (Ed.). (2010). *The economics of ecosystems and biodiversity: Ecological and economic foundations*. Earthscan.

Lilieholm, R. J. (2007). Forging a common vision for Maine's North Woods. *Maine Policy Review, 16*(2), 12–25. https://doi.org/10.53558/EXAQ5460

Michailakis, D., & Schirmer, W. (2014). Social work and social problems: A contribution from systems theory and constructionism. *International Journal of Social Welfare, 23*(4), 431–442. https://doi.org/10.1111/ijsw.12091

Olawoyin, W. K., & Lamidi, K. O. (2019). Investigating ICT usage and transparency in governance processes at the local level in Southwestern Nigeria. *Journal of Governance and Public Policy, 6*(2), 148–169.

Phillips, A. (Ed.). (1998). *Economic values of protected areas: Guidelines for protected area managers*. IUCN.

Republic of South Africa. (2013). *Protection of Personal Information Act 4 of 2013*. Government Gazette No. 37067. https://www.gov.za/documents/protection-personal-information-act

Sikder, A. K., Aksu, H., & Uluagac, A. S. (2020). *A context-aware framework for detecting sensor-based threats on smart devices*. IEEE Transactions on Mobile Computing, 19(2), 245–261. https://doi.org/10.1109/TMC.2019.2893253

Taiwo, I. O., Ibitoye, M. O., Oladejo, S. O., & Koeva, M. (2024). *Fitness of multi-resolution remotely sensed data for cadastral mapping in Ekiti State, Nigeria. Remote Sensing, 16*(19), 3670. https://doi.org/10.3390/rs16193670

Tietenberg, T. H., & Lewis, L. (2016). *Environmental and natural resource economics* (10th ed.). Routledge.

Ugonabo, C. U., Egolum, C. C., & Sado, R. O. (2023). *Nigerian land policy: Issues, challenges and the way forward. Global Journal of Politics and Law Research, 11*(4), 57–77. https://doi.org/10.37745/gjplr.2013/vol11n45777

Von Solms, R., & Van Niekerk, J. (2013). *From information security to cyber security*. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Watson, J. E. M., Dudley, N., Segan, D. B., & Hockings, M. (2014). The performance and potential of protected areas. *Nature, 515*(7525), 67–73.