ISSN 2616-7433 Vol. 7, Issue 7: 61-68, DOI: 10.25236/FSST.2025.070710

Artificial Intelligence Oriented Landscape Design and Ecological Security Network Space Reconstruction Strategy for Urban and Rural Integration Area

Xuan Wang[1,a], Jingxin Guan[1,b,*]

[1]School of Construction, Guangdong Polytechnic College, Zhaoqing, Guangdong, China
[a]3037589165@qq.com, [b]1341572250@qq.com
[*]Corresponding author

Abstract: *Urban-rural integration represents the pinnacle of rural social development, serving both as an aspirational goal and a driver of spatial production. Concurrently, escalating cyber threats challenge traditional security models, especially for critical infrastructure. This study investigates landscape design and ecological-security-oriented cyberspace reconstruction within integrated urban-rural contexts. It synthesizes scholarly discourse on these two focal themes and examines AI's (Artificial Intelligence) role in securing public cloud IoT authentication. An algorithmic framework is established, proposing multiple AI-driven models to theoretically underpin landscape design and cyberspace resilience strategies in integrated regions. The paper further conceptualizes AI's function in shaping landscape aesthetics and cyberspatial governance. Simulation experiments validate the models: AI-enhanced security systems outperformed conventional defenses by 1.2% in average efficacy. The process value for ecological source quality increased from 7 in Phase I to 46 in Phase IV, demonstrating a substantial improvement. As AI and IoT evolve, urban management confronts transformative opportunities and complex challenges. This research bridges physical landscape planning with digital ecological security, offering an interdisciplinary, AI-informed approach to sustainable urban-rural development amid growing cyber-physical interdependencies.*

Keywords: *Ecological Security, Landscape Design, Internet of Things, Artificial Intelligence*

1. Introduction

The rapid development of urban-rural integration areas often overlooks existing ecological foundations, leading to issues such as blurred rural identity, fragmented landscapes, and ecological imbalance. Concurrently, accelerated urbanization intensifies conflicts among land use, transportation, and ecology, posing significant threats to sustainable development.

Scholars have extensively examined AI-oriented landscape design in urban-rural integration contexts. Key evaluation factors for urban and rural space quality have been identified, including landscape coordination and cultural awareness [1]. AI and street-level imagery have been combined to advance urban landscape research [2], while big data, AI, and IoT have been shown to reshape urban governance and infrastructure management [3]. Neural networks have been applied to model species diversity in response to urbanization [4], and integrated models have been proposed to simulate 3D urban expansion [5]. Studies have also explored water-sensitive planning for coordinated landscape and economic development [6], emphasized IoT and AI as foundations of smart cities [7], and highlighted the importance of locally grounded landscape sustainability science [8]. Despite these advances, challenges remain as technology evolves.

Research has also explored AI's role in reconstructing ecological security in cyberspace. Mathew Alex described the dual role of AI in cybercrime and defense, highlighting its use in building adaptive security systems [9]. Qiu Jing noted that AI enhances cybersecurity capabilities but also introduces new risks through autonomous learning from large datasets [10]. Morrison M. Irene explored AI-based approaches to improving network protection [11]. Wirkuttis Nadine emphasized AI's capacity for real-time processing of massive dynamic data to support intelligent defense [12], while Nainggolan Dicky RM argued that AI surpasses traditional security technologies by offering effective responses to diverse vulnerabilities [13]. Samtani Sagar analyzed the distinctive characteristics of AI-based cybersecurity as an emerging discipline [14]. Collectively, these studies confirm AI's beneficial impact

ISSN 2616-7433 Vol. 7, Issue 7: 61-68, DOI: 10.25236/FSST.2025.070710

while acknowledging persistent challenges.

This paper examines landscape design in urban-rural integration areas and proposes a reconstruction strategy for ecological security cyberspace under AI. It begins by analyzing AI in relation to landscape style and cyberspace concepts. Design recommendations are then provided for construction, waterscape, and pavement elements, alongside detailed segmentation of safety network frameworks and ecological source quality. By evaluating four AI-related algorithms within defense and security systems, the study formulates a reconstruction strategy for ecological security cyberspace, offering a reference for future research in this field.

2. AI Related Concepts in Landscape and Cyberspace

(1) Landscape

Landscape style encompasses a region's natural landforms and scenic character, functioning as both a basic spatial unit and a perceptual-geographic entity. "Landscape" denotes spaces with aesthetic, visual, and psychological value, while "style" refers to outward form shaped by material and immaterial factors. Though no unified definition exists, this paper conceptualizes landscape as an aesthetic space embodying both form and artistic conception—simultaneously material and immaterial. Landscape style analysis is illustrated in Figure 1.

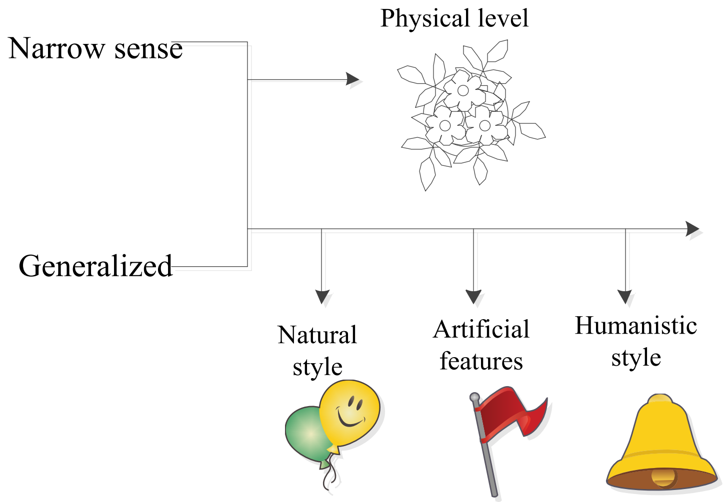

Figure 1 Concept analysis of landscape style

(2) Ecological security cyberspace

Cyber Security (CS) refers to ensuring that the hardware, software, and associated components of a network system are not damaged or altered by accidental or malicious causes, thereby guaranteeing continuous, stable, normal, and uninterrupted operation.

Computer Communication Network Security, as a core component of CS, pertains to securing data exchange among independent computers interconnected via communication devices, transmission media, and software, and enabling resource sharing across geographically distributed systems through communication protocols — with the communication network being the primary enabler of such sharing. Security here requires that the communication network meets user demands. In the following discussion, "Cyber Security" encompasses both computer network and computer communication network security.

3. Methods of AI in Landscape Design and Ecological Security Network Space Reconstruction Strategy of Urban and Rural Integration Area

(1) AI landscape design in urban and rural integration area

The landscape design content of three AI points in urban and rural integration area is summarized, as shown in Figure 2.

ISSN 2616-7433 Vol. 7, Issue 7: 61-68, DOI: 10.25236/FSST.2025.070710

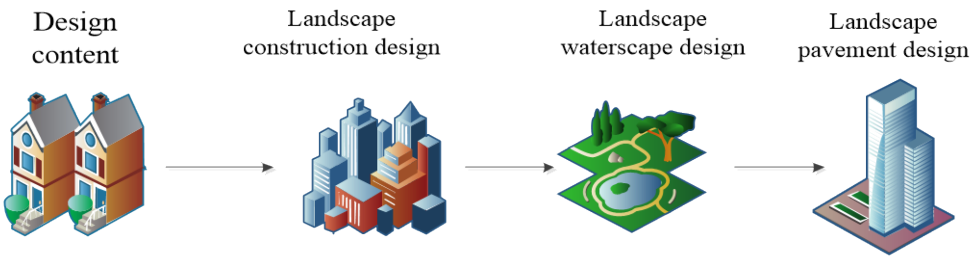

Figure 2 Landscape design of artificial intelligence in urban-rural integration areas

1) Impact of AI on landscape construction design

AI elevates architectural elements in landscape design by enabling precision planning and creative expansion. Through computational color and pattern synthesis, it boosts aesthetic diversity while preserving functionality and artistry — empowering designers with richer tools and raising design standards. Example: AI-assisted façade design enhances both scientific rigor and stylistic uniqueness.

2) Impact of AI on landscape waterscape design

AI transforms waterscapes from static features into dynamic, multisensory experiences. Synchronized fountains, responsive lighting, and laser projections merge water, sound, and light — enhancing visual drama, ecological integration, and audience interaction. These innovations are now widely deployed in contemporary landscape projects.

3) Impact of AI on landscape pavement design

AI redefines pavement aesthetics through intelligent color, pattern, and material optimization — increasing visual richness and spatial clarity. Projected imagery and embedded LED lighting create immersive, luminous surfaces that amplify atmospheric depth and sensory engagement, effectively translating design intent into experiential impact.

(2) AI reconstruction strategy in ecological security cyberspace

The two AI reconstruction strategies in the ecological security cyberspace are summarized, as shown in Figure 3.

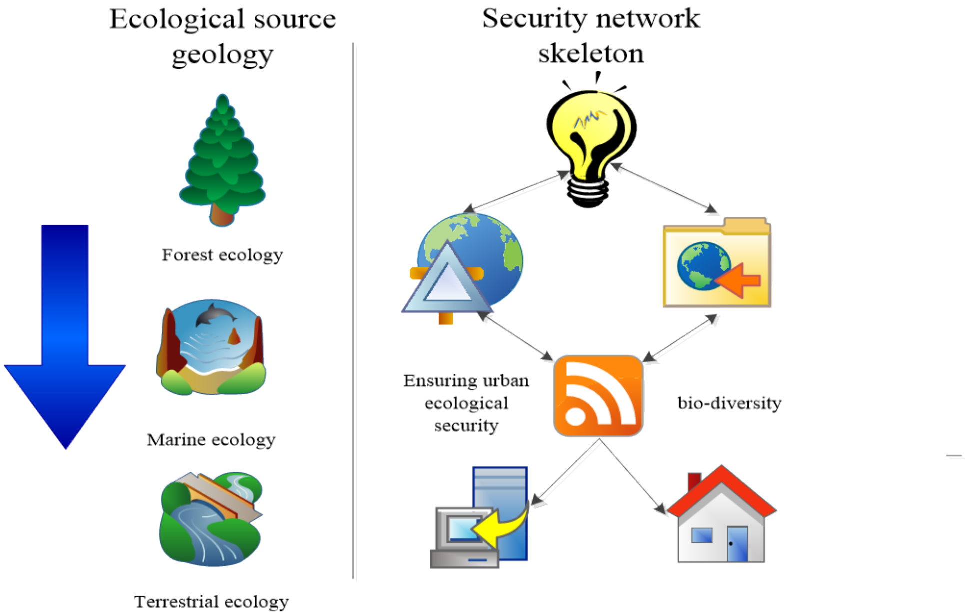

Figure 3 Reconstruction strategy of artificial intelligence in ecological security cyberspace

1) Construction of landscape ecological security network framework

The ecological security model shows that the connectivity and cross structure characteristics of

ISSN 2616-7433 Vol. 7, Issue 7: 61-68, DOI: 10.25236/FSST.2025.070710

China's urban ecological security networks are significantly different in space, and present an uneven distribution pattern. In order to ensure urban ecological security, maintain biodiversity and optimize urban ecological structure, it is necessary to carry out the development and exploitation of various ecological resources as early as possible.

2) Improvement of ecological source quality

This paper proposes measures based on the spatial structure and distribution of regional ecosystems to strengthen green barriers, reduce ecological pressure, and improve water quality. Forests, gardens, lakes, and reservoirs serve as core ecological sources and key supports for urban ecological security. In some areas, cultivated land, orchards, and forests, interspersed with towns, industrial zones, and villages, are highly vulnerable to degradation, increasing environmental stress. Strict land use control and enhanced rural landscape protection are needed to promote urban ecological agriculture. Mountain forests and gardens should be reinforced to form a central green corridor connecting northern and southern ecosystems. Ecological sources also include seas, lakes, reservoirs, and ponds. Management should focus on intertidal zones, aquaculture areas, mangroves, and artificial beaches, while protecting lake shorelines, pond bases, and island vegetation to gradually restore submerged aquatic vegetation in lakes.

(3) Application of AI in the safe and efficient authentication of public cloud Internet of Things

IoT devices can collect data through a large number of sensors. AI can help IoT devices analyze massive data in a very short time. Although it has many devices and sensors, its integration with the Internet makes it have higher visibility and control. AI can turn the information obtained from the Internet of Things into useful information. This is particularly important to prevent devices and networks from being accessed and intruded illegally, as shown in Figure 4.

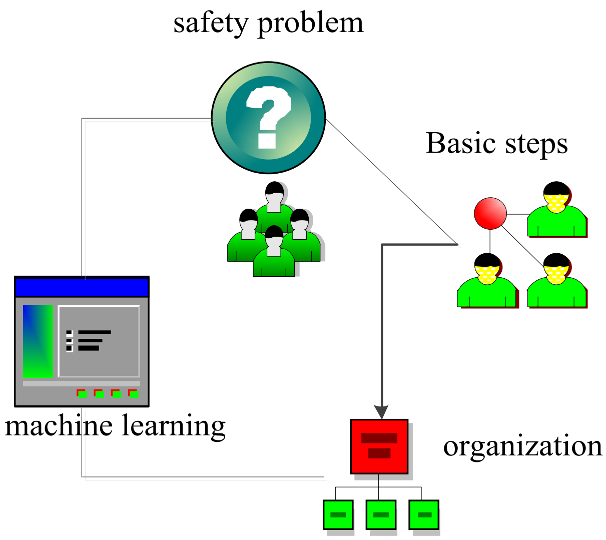

Figure 4 Application of artificial intelligence in the security and efficient authentication of public Cloud Internet of Things

1) Security issues in the Internet of Things

Multiple factors affect CS, presenting significant challenges for IoT devices. The field encompasses a wide range of devices, each with its own operating system and security weaknesses, making it impossible for a single defense system to provide full coverage. Due to low design costs, most IoT devices are energy efficient and lack embedded security frameworks. Networks typically involve thousands of such devices transmitting data, rendering security highly unpredictable. To manage this, networks must ensure all operating systems and applications can be updated, maintain reserves of new resources, perform security evaluations, and detect potential attack targets.

2) AI in IoT CS

To establish a security architecture of the Internet of Things, the key is to identify all devices in the entire network. This is a huge challenge for a huge network with millions of sensors and devices. However, with the help of AI, the discovery program is simpler and can fully understand the

ISSN 2616-7433 Vol. 7, Issue 7: 61-68, DOI: 10.25236/FSST.2025.070710

characteristics of this device. Effective CS is to identify and monitor each node, and AI's identification and asset management capabilities enable it to protect network security [15].

Data analysis can be used to provide security for the Internet of Things. AI does not feel tired. It can better monitor the large-scale Internet of Things network to find abnormal behavior. Machine learning techniques can be used and AI can be trained to determine attack patterns. Due to personal privacy, the vulnerability information generated by real attacks is rarely disclosed, so that the analysis quality of each time is limited.

3) Application of machine learning in the Internet of Things

Machine learning can detect potential threats, identify network flaws, and uncover security vulnerabilities such as weak or missing passwords on IoT devices, enabling proactive defense through network configuration. Although the use of large-scale CS and IoT data raises security concerns for many companies, machine learning has been shown to effectively resist DDoS (Distributed denial of service) attacks and strengthen the security of the entire IoT network. Early threat detection also helps manufacturers design more secure products and deploy security patches in a timely and efficient manner.

4. AI Related Application Algorithm

(1) Standardized method

To eliminate dimensional differences among evaluation indices, the range standardization method was applied:

$$X_{nm} = \frac{X_{nm} - X_{nm}\min}{X_{nm}\max - X_{nm}\min} \tag{1}$$

$$X_{nm} = \frac{X_{nm}\max - X_{nm}}{X_{nm}\max - X_{nm}\min} \tag{2}$$

Among them: X_{nm}, $X_{nm}\max$ and $X_{nm}\min$ are the actual value, maximum value and minimum value of the m index in the nth sample area respectively.

(2) Index calculation method

Topographic factors were integrated into a comprehensive geomorphic factor:

$$T = \lg[(E/E'+1)+(S/S'+1)] \tag{3}$$

In the formula, E is the height of the grid. E' is the average altitude of the study area. S is the slope of the grid. S' is the average slope of the study area.

$$W = \sum w_i \times A_i / A_r \tag{4}$$

The landscape dominance was evaluated using the largest patch index:

$$L = \max(A_{Ei},\ldots,A_{En})/A_R \tag{5}$$

The road barrier of various areas is:

$$R = \sum RI_i \times L_i / A_R \tag{6}$$

5. Simulation Experiment of Landscape Design and Ecological Security Cyberspace Reconstruction Strategy in Urban and Rural Integration Area

(1) Content of landscape design in the fusion area

Through the waterscape design, construction design and pavement design of the four fusion areas A, B, C and D, as shown in Figure 5.

ISSN 2616-7433 Vol. 7, Issue 7: 61-68, DOI: 10.25236/FSST.2025.070710

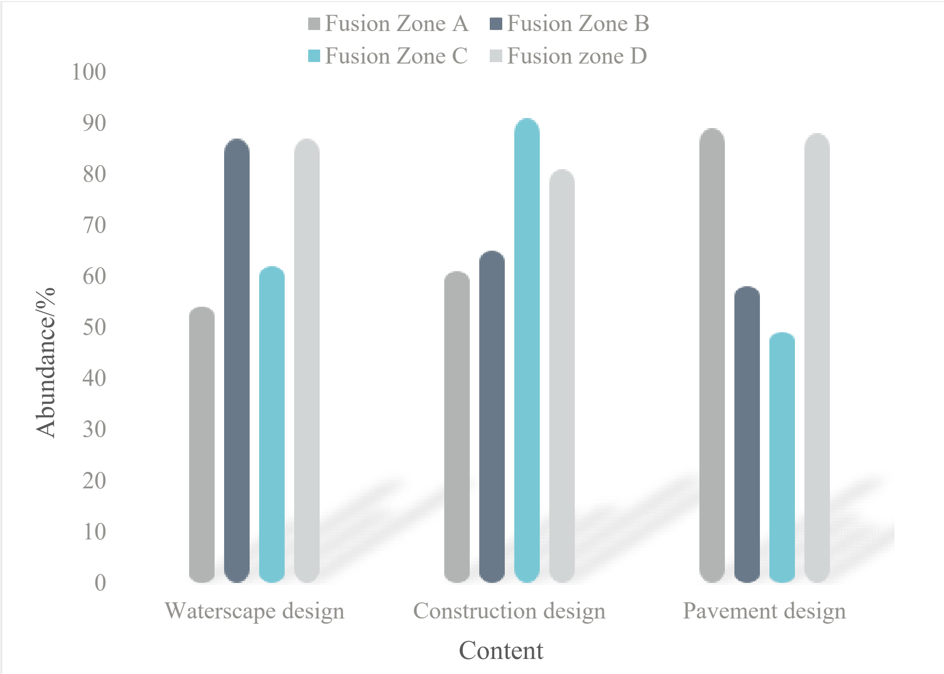

Figure 5 Content analysis of the landscape style design in the fusion area

Figure 5 reveals varying levels of design richness across four integration zones. In Zone A, waterscape, construction, and pavement richness are 54%, 61%, and 89%, respectively; in Zone B, 87%, 65%, and 58%; in Zone C, 62%, 91%, and 49%; and in Zone D, 87%, 81%, and 88%. In Zones A to C, one design type dominates: pavement in A, waterscape in B, and construction in C. Zone D exhibits uniformly high richness, with all three elements exceeding 80%. Average richness values are 68% for Zone A, 70% for Zone B, 67.3% for Zone C, and 85.3% for Zone D.

(2) Strategy of ecological security network space reconstruction

Based on the above content analysis of security network framework and ecological source quality, the four phases of cyberspace reconstruction are analyzed and the process value is 1-100, as shown in Figure 6.

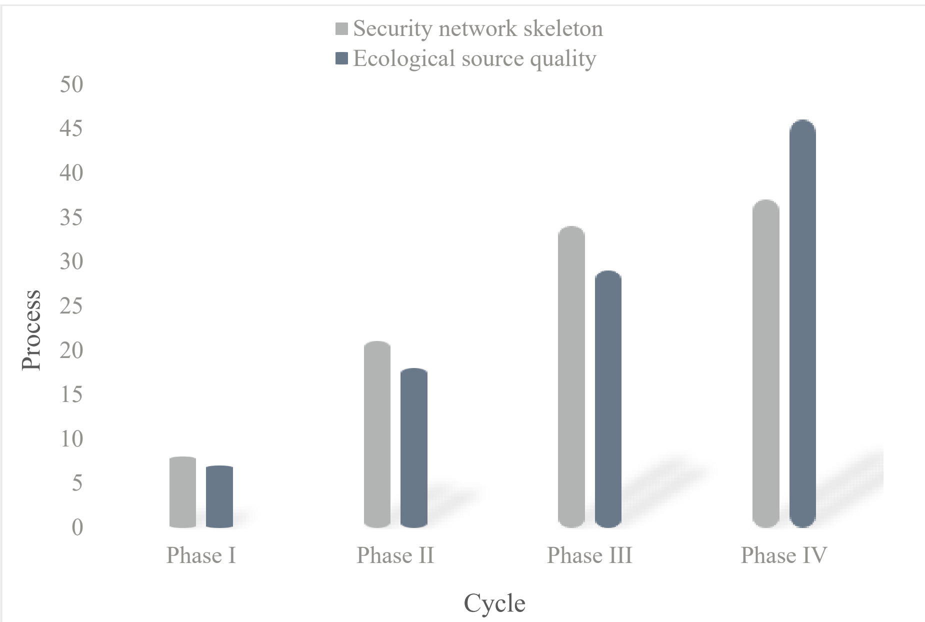

Figure 6 Analysis of ecological security cyberspace reconstruction strategy

It can be seen from Figure 6 that the security framework and ecological source quality in the ecological security cyberspace reconstruction strategy have a certain development law in the four

ISSN 2616-7433 Vol. 7, Issue 7: 61-68, DOI: 10.25236/FSST.2025.070710

phases of the cycle. Generally, the process value increases gradually from Phase I to Phase IV to reach the maximum. In the security network framework, the process value of Phase I is 8, and the process value of Phase IV is 29 higher than that of Phase I. In the quality of ecological source area, the process value of Phase I is 7, and the process value of Phase IV is 39 higher than that of Phase I.

(3) Application of AI algorithm in security network space reconstruction

AI related algorithms include: Convolutional Neural Networks (CNN), Naive Bayesian Model (NBM), Random Forest (RF), Machine Learning Algorithm (MLA). The listed four AI related algorithms are used to analyze the effectiveness of applications in security network space reconstruction, as shown in Figure 7.

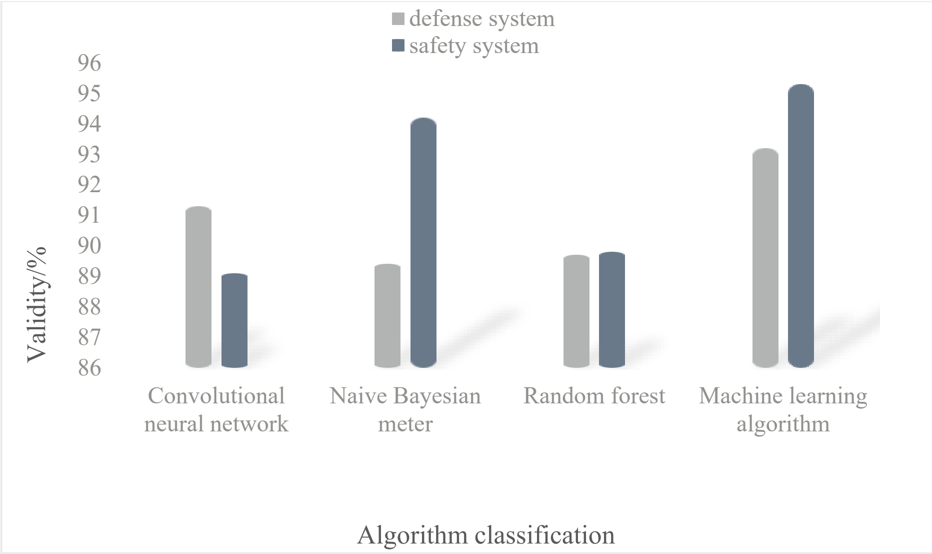

Figure 7 Application of artificial intelligence algorithm in secure network space reconstruction

Figure 7 shows that among the four AI algorithms, the machine learning algorithm (MLA) achieves the highest effectiveness in constructing a secure cyberspace. In the defense system, CNN, NBM, RF, and MLA attain effectiveness rates of 91.3%, 89.4%, 89.7%, and 93.2%, respectively. In the security system, their effectiveness is 89.1%, 94.2%, 89.8%, and 95.3%, respectively, confirming MLA's superior performance in both systems. As noted earlier, machine learning is particularly valuable for configuring network defenses. The average effectiveness across all four algorithms is 90.9% in the defense system and 92.1% in the security system, indicating that AI performs 1.2% better on average in the security system.

In summary, this paper investigates AI oriented landscape design in urban rural integration areas and strategies for reconstructing ecological security cyberspace through simulation experiments. The study proceeds along three dimensions: analysis of landscape design in the integration zone, reconstruction strategies for ecological security cyberspace, and application of AI algorithms in this reconstruction. Results show that AI algorithms perform more effectively, on average, in the security system than in the defense system.

6. Conclusion

From an urban-rural integration perspective, this paper investigates urban-rural and regional imbalances. Integrating landscape ecology into urban planning enhances urban livability and supports environmental protection, contributing positively to urban development. By analyzing a landscape ecological security model, the study applies it to public cloud authentication and derives a corresponding ecological security network reconstruction strategy. Results indicate that randomly distributed ecological source areas possess a robust ecological security foundation.

Acknowledgments

This work was supported by 2023YBSK020.

ISSN 2616-7433 Vol. 7, Issue 7: 61-68, DOI: 10.25236/FSST.2025.070710

References

[1] Xu, Tingting, Giovanni Coco, and Jay Gao. "Extraction of urban built-up areas from nighttime lights using artificial neural network." Geocarto International 35.10 (2020): 1049-1066.

[2] Li, Xiaojiang, Bill Yang Cai, and Carlo Ratti. "Using street-level images and deep learning for urban landscape studies." Landscape Architecture Frontiers 6.2 (2018): 20-30.

[3] Engin, Zeynep. "Data-driven urban management: Mapping the landscape." Journal of Urban Management 9.2 (2020): 140-150.

[4] Pourmohammad, Parisa. "Road impact assessment modelling on plants diversity in national parks using regression analysis in comparison with artificial intelligence." Modeling Earth Systems and Environment 6.3 (2020): 1281-1292.

[5] He, Qingsong. "Simultaneously simulate vertical and horizontal expansions of a future urban landscape: A case study in Wuhan, Central China." International journal of geographical information science 31.10 (2017): 1907-1928.

[6] Allam, Zaheer, Houriiyah Tegally, and Meelan Thondoo. "Redefining the use of big data in urban health for increased liveability in smart cities." Smart Cities 2.2 (2019): 259-268.

[7] Deng, Tianhu, Keren Zhang, and Zuo-Jun Max Shen. "A systematic review of a digital twin city: A new pattern of urban governance toward smart cities." Journal of Management Science and Engineering 6.2 (2021): 125-134.

[8] Liao, Chuan. "Advancing landscape sustainability science: theoretical foundation and synergies with innovations in methodology, design, and application." Landscape ecology 35.1 (2020): 1-9.

[9] Mathew, Alex. "Artificial intelligence for offence and defense-the future of cybersecurity." Educational Research 3.3 (2021): 159-163.

[10] Qiu, Jing. "Artificial intelligence security in 5G networks: Adversarial examples for estimating a travel time task." IEEE Vehicular Technology Magazine 15.3 (2020): 95-100.

[11] Morrison, M. Irene. "Info-topia: Postcolonial cyberspace and artificial intelligence in TRON: Legacy and Nalo Hopkinson’s Midnight Robber." Journal of Postcolonial Writing 54.2 (2018): 161-173.

[12] Wirkuttis, Nadine, and Hadas Klein. "Artificial intelligence in cybersecurity." Cyber, Intelligence, and Security 1.1 (2017): 103-119.

[13] Nainggolan, Dicky RM. "Data Science, Big Data, and Predictive Analytics: a Platform for Cyberspace Security Intelligence." Jurnal Pertahanan & Bela Negara 7.2 (2017): 19-36.

[14] Samtani, Sagar, Murat Kantarcioglu, and Hsinchun Chen. "Trailblazing the artificial intelligence for cybersecurity discipline: a multi-disciplinary research roadmap." ACM Transactions on Management Information Systems (TMIS) 11.4 (2020): 1-19.

[15] Kavitha, S."An internet of things for data security in cloud using artificial intelligence." International Journal of Grid and Distributed Computing 14.1 (2021): 1257-1275.