Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Predictive Analytics and Autonomous Decision-Making: AI's Role in Enterprise Network Management for Smart Buildings

Jithendra Babu Punugubati
JNTU Hyderabad, India
Corresponding Author: Jithendra Babu Punugubati, **E-mail**: jithendrababup@gmail.com

| ABSTRACT

Artificial intelligence has fundamentally transformed enterprise network management within smart building ecosystems, creating unprecedented opportunities for automation, optimization, and security enhancement. This integration enables networks to autonomously classify diverse traffic patterns, apply appropriate quality of service policies, and detect anomalous activities without continuous human intervention. The symbiotic relationship between AI systems and network engineers facilitates intent-based configuration, where high-level objectives translate into granular network adjustments. Smart buildings particularly benefit from this technological convergence as network-generated data informs environmental controls, occupancy management, and energy utilization. The resulting dynamic infrastructure demonstrates greater resilience, adaptability, and efficiency than traditional network architectures, while simultaneously reducing operational complexity. As building systems grow increasingly interconnected, this AI-enhanced network intelligence serves as the critical foundation for next-generation smart infrastructure development, enabling buildings to respond intelligently to changing conditions while maintaining optimal performance.

| KEYWORDS

Enterprise networks, artificial intelligence, smart buildings, network automation, quality of service

| ARTICLE INFORMATION

ACCEPTED: 01 June 2025 **PUBLISHED:** 23 June 2025 **DOI:** 10.32996/jcsts.2025.7.107

1. Introduction to AI in Enterprise Network Management

Enterprise networks have undergone a profound transformation with the integration of artificial intelligence technologies, revolutionizing how network infrastructure is managed, monitored, and optimized. AI applications in network management have enabled predictive capabilities that were previously unattainable through conventional methods [1]. This paradigm shift comes at a critical moment as smart building infrastructures grow increasingly complex, incorporating numerous interconnected systems from environmental controls to security apparatus, all competing for network resources.

1.1 Overview of AI's Impact on Enterprise Networks

The impact of artificial intelligence on enterprise networks extends across multiple dimensions, from operational efficiency to security posture. Network management systems enhanced with AI can continuously analyze vast quantities of telemetry data, identifying patterns and anomalies that would remain undetectable through manual monitoring. These capabilities have transformed reactive network management into proactive optimization, where potential issues are identified and remediated before affecting users or services. The implementation of machine learning algorithms for load prediction in IEEE 802.11 networks demonstrates how AI can anticipate network demands and proactively allocate resources to maintain optimal performance [1].

1.2 Current Landscape of Smart Building Network Complexity

The current landscape of smart building networks presents unprecedented challenges in terms of scale, heterogeneity, and dynamic requirements. Modern enterprise environments must support diverse systems including Internet of Things (IoT) sensors, building automation controls, security cameras, access systems, and traditional IT services—all with varying demands for bandwidth, latency, and reliability. This complexity necessitates intelligent systems capable of understanding and adapting to the interconnected nature of smart building ecosystems [2]. The creation of truly smart buildings requires networks that can dynamically adjust to changing conditions and usage patterns while maintaining service quality across all connected systems.

1.3 Need for Advanced Management Solutions Beyond Manual Intervention

Manual network management approaches have reached their practical limits in these environments. Network engineers can no longer effectively monitor, troubleshoot, and optimize these multifaceted systems using traditional techniques alone. The sheer volume of devices, connections, and potential configuration permutations exceeds human cognitive capacity, creating an imperative for AI-augmented solutions that can process vast quantities of network telemetry data and extract actionable insights. As smart buildings continue to evolve in complexity, the necessity for automated, intelligent management systems becomes increasingly apparent [2].

1.4 Introduction to AI-driven Network Analytics Platforms

Leading technology providers have responded to these challenges with sophisticated AI-driven network analytics platforms. Cisco Digital Network Architecture (DNA) represents one comprehensive solution, offering capabilities for network assurance, automation, and security through machine learning algorithms that continuously analyze network behavior. Similarly, Aruba AIOps leverages artificial intelligence for operations to detect anomalies, predict issues before they impact users, and recommend remediation steps based on learned patterns across the network infrastructure. These platforms exemplify how AI is becoming an essential component of enterprise network management, particularly in the context of smart building environments where operational continuity and performance optimization are paramount concerns [1].

Feature	Traditional Approach	AI-Enhanced Approach	Key Benefit
Traffic Analysis	Manual threshold monitoring	Automated pattern recognition	Early problem detection
Configuration	Manual updates	Intent-based automation	Reduced errors
Anomaly Detection	Signature-based	Behavioral analysis	Zero-day threat identification
Load Prediction	Static capacity planning	Dynamic resource allocation	Optimized performance
Network Assurance	Reactive troubleshooting	Proactive issue prevention	Improved uptime

Table 1: Comparison of AI-Driven Network Analytics Platforms for Smart Buildings [1, 9]

2. Automated Traffic Classification and Quality of Service

Enterprise networks in smart building environments face increasing challenges in managing diverse traffic types with varying requirements. The application of artificial intelligence to traffic classification and Quality of Service (QoS) management represents a significant advancement in addressing these challenges. Intelligent systems now enable networks to automatically identify different traffic categories and apply appropriate policies without manual configuration.

2.1 AI Mechanisms for Distinguishing Between Traffic Types

Modern enterprise networks must efficiently handle multiple traffic categories including surveillance video streams, Voice over IP (VoIP) communications, building automation control signals, and standard user traffic. Traditional static classification methods have proven insufficient for the dynamic nature of contemporary network environments. Machine learning approaches have emerged as powerful tools for accurate traffic identification. Supervised learning algorithms analyze packet characteristics, flow behaviors, and temporal patterns to classify traffic with high precision [3]. Deep learning models particularly excel at recognizing subtle differences between traffic types, adapting to changing application signatures, and identifying encrypted traffic based on behavioral patterns rather than packet inspection. These classification mechanisms operate continuously, learning from network behaviors and improving accuracy over time.

Traffic Type	Primary Classification Method	QoS Priority	Key Requirement
Video Surveillance	Flow behavior analysis	High	Consistent bandwidth
VoIP Communications	Packet pattern recognition	Very high	Minimal latency
Building Automation	Protocol identification	Medium	Low jitter
IoT Sensor Data	Behavioral fingerprinting	Low	Reliability
User Applications	Application signatures	Variable	Adaptability

Table 2: Classification Methods for Different Network Traffic Types [3, 4]

2.2 Dynamic QoS Policy Application Based on Traffic Classification

The automatic classification of network traffic enables intelligent Quality of Service management through dynamic policy application. Once traffic is correctly identified, AI systems can automatically implement appropriate QoS policies that align with business priorities and technical requirements. This represents a significant advancement from static QoS configurations that required manual adjustment. Dynamic QoS systems continuously evaluate network conditions and traffic patterns, adjusting priority levels, bandwidth allocations, and queuing strategies in real-time [4]. These adjustments ensure critical applications receive necessary resources even as network conditions fluctuate. The architecture for dynamic management of QoS policies has proven particularly valuable in heterogeneous network environments where traffic patterns and priorities frequently change based on time of day, occupancy levels, or business activities.

2.3 Impact on Real-time and Latency-Sensitive Applications

Latency-sensitive applications such as building security systems, emergency communications, and environmental controls require consistent performance to function correctly. AI-driven traffic classification and QoS management significantly improve the reliability of these critical systems. By accurately identifying time-sensitive traffic and assigning appropriate priorities, AI systems ensure that critical applications receive necessary network resources even during periods of congestion [3]. This capability proves especially valuable for applications like video surveillance that require both low latency and high bandwidth. Voice communications benefit from reduced jitter and packet loss, while building control systems gain improved responsiveness and reliability. The overall impact extends beyond performance improvements to enhanced safety, security, and operational efficiency throughout smart building environments.

2.4 Case Studies of Successful Implementations

Numerous organizations have successfully deployed AI-driven traffic classification and QoS management systems with measurable benefits. Large corporate campuses have implemented these technologies to balance competing demands between IoT sensors, security systems, and user applications [4]. Healthcare facilities have deployed intelligent classification systems to ensure medical devices and emergency communications receive priority over administrative traffic. Educational institutions have utilized AI-driven QoS to maintain consistent performance for distance learning applications while accommodating research needs and administrative functions. These implementations demonstrate significant improvements in application performance, network reliability, and user satisfaction compared to traditional management approaches. The success of these deployments provides valuable insights into best practices for implementation and tuning of AI-driven traffic management systems in diverse enterprise environments.

3. Intelligent Anomaly Detection for Network Security

The integration of artificial intelligence into network security operations has revolutionized the detection and response to potential threats in enterprise environments. As smart buildings incorporate increasingly complex systems with numerous access points, traditional security approaches have proven inadequate. AI-powered anomaly detection provides a sophisticated solution that adapts to evolving threats while reducing false positives and operational overhead.

3.1 AI Approaches to Identifying Unusual Network Patterns

Artificial intelligence has transformed anomaly detection by enabling systems to establish behavioral baselines and identify deviations that may indicate security threats. Machine learning algorithms analyze historical network data to understand normal operational patterns and detect subtle anomalies that would escape traditional rule-based systems. Deep learning approaches have proven particularly effective at identifying complex patterns in network traffic without requiring manual feature engineering [5]. Unsupervised learning techniques can discover previously unknown threat patterns, while supervised methods excel at classifying known attack signatures with high accuracy. Generative Adversarial Networks represent an advanced approach where two competing neural networks simultaneously improve detection capabilities and reduce false positives through an evolutionary process. These AI techniques continuously refine their understanding of normal network behavior, adapting to changing conditions without requiring constant reconfiguration.

3.2 Detection Capabilities for Switch Port Activity, Bandwidth Spikes, and Unauthorized Access

AI-powered security systems monitor multiple dimensions of network activity to provide comprehensive threat detection. At the switch port level, intelligent systems track connection patterns, MAC address changes, and traffic characteristics to identify potential compromise or unauthorized device connections. Bandwidth analysis algorithms detect anomalous spikes or unusual traffic flows that may indicate data exfiltration attempts or denial-of-service attacks [6]. User access monitoring employs behavioral biometrics to identify potentially compromised credentials based on deviations from established usage patterns. Enhanced feature engineering approaches have significantly improved detection accuracy by incorporating contextual information from multiple data sources. This multi-dimensional monitoring provides defense-in-depth that addresses both external threats and potential insider attacks across the network infrastructure.

3.3 Comparison with Traditional Security Monitoring Approaches

Traditional network security monitoring relied primarily on signature-based detection and static rule sets that required constant updating and generated numerous false positives. These approaches struggled to identify novel threats and required significant human intervention for tuning and analysis. In contrast, AI-based systems can detect zero-day attacks by identifying behavioral anomalies rather than matching known signatures [5]. Machine learning models adapt to network changes without manual reconfiguration, reducing maintenance requirements while improving detection capabilities. The dataset-driven approach to network anomaly detection in Industrial Internet of Things environments has demonstrated superior performance compared to conventional methods [6]. While traditional systems focus primarily on known threat patterns, AI-powered solutions balance signature recognition with behavioral analysis to provide comprehensive protection against both known and emerging threats.

3.4 Quantifiable Improvements in Security Posture and Network Uptime

Organizations implementing AI-powered anomaly detection have reported significant improvements in their overall security posture and operational efficiency. Detection times for potential threats have decreased substantially compared to traditional approaches, with many attacks identified during reconnaissance phases before damage occurs [5]. False positive rates have declined dramatically, allowing security teams to focus resources on legitimate threats rather than investigating benign anomalies. Network uptime has improved through early detection of performance issues that might otherwise escalate to service disruptions. Mean time to resolution for security incidents has decreased as AI systems provide contextualized alerts with actionable intelligence rather than isolated data points. These improvements translate directly to enhanced protection for critical infrastructure, reduced operational costs, and improved compliance with security regulations and standards. The combined benefits of enhanced detection capabilities and operational efficiencies demonstrate the transformative impact of AI on network security in enterprise environments.

4. Smart Building Optimization Through Network Intelligence

The convergence of network intelligence and building management systems represents a significant advancement in smart building optimization. Modern enterprise networks generate substantial data about usage patterns, device connections, and traffic flows that—when properly analyzed—provide valuable insights for building operations. Artificial intelligence transforms this network data into actionable intelligence that enhances occupant comfort, improves energy efficiency, and optimizes resource allocation across building systems.

4.1 Correlation Between Network Data and Building Occupancy Patterns

Enterprise networks serve as rich sources of information about building occupancy and usage patterns. WiFi connection data, network authentication logs, and switch port activity collectively provide detailed insights into when and where occupants are present throughout a facility. Sophisticated AI algorithms can process this network information to develop highly accurate occupancy models without requiring dedicated occupancy sensors. Smartphone-based indoor positioning systems offer particularly valuable data for multi-floor occupancy detection, enabling precise tracking of movement patterns throughout complex buildings [7]. This network-derived occupancy intelligence serves as a foundation for numerous optimization strategies, from environmental controls to security operations. The ability to understand occupancy patterns with temporal and spatial precision enables building systems to anticipate needs rather than simply reacting to conditions, creating more responsive and efficient environments.

4.2 AI-Driven Environmental Control Adjustments

Network intelligence enables environmental systems to anticipate occupant needs and optimize comfort while minimizing energy consumption. AI algorithms analyze historical occupancy data alongside real-time network information to predict when specific areas will be occupied, allowing HVAC systems to precondition spaces just before use rather than operating continuously. Lighting systems leverage network-derived presence information to adjust illumination levels based on actual usage rather than scheduled operations. Conference room environmental controls can automatically adjust based on the number of attendees detected through network connections. These intelligent adjustments create environments that respond dynamically to changing occupancy conditions while eliminating waste from conditioning unoccupied spaces. The integration of AI for energy management in building systems represents a vertical application domain that delivers substantial efficiency improvements [8].

Application	Network Data Source	Building System Impact
Occupancy Detection	WiFi connections, authentication	HVAC optimization
Energy Management	Traffic patterns, device connections	Consumption reduction
Space Utilization	Connection density, duration	Facilities planning
Security Operations	Access patterns, anomalies	Enhanced physical security
Meeting Room Optimization	Connection counts, patterns	Improved scheduling

Table 3: Network-Derived Building Intelligence Applications [7, 8]

4.3 Energy Usage Optimization Methodologies

Network-informed energy optimization extends beyond simple occupancy-based controls to comprehensive methodologies that balance multiple variables. AI systems analyze patterns of energy consumption in relation to network activity, identifying opportunities for load shifting, peak demand reduction, and equipment scheduling optimization. Computational intelligence techniques enable predictive energy management that accounts for factors including weather forecasts, occupancy predictions, and equipment efficiency profiles. These methodologies optimize energy consumption while maintaining or improving occupant comfort and productivity. The IEEE Computational Intelligence Society has recognized energy optimization as a critical vertical application domain for artificial intelligence, highlighting its importance for sustainable building operations [8]. By correlating network data with energy consumption patterns, AI systems create optimization strategies that would be impossible through conventional building management approaches.

4.4 Machine Learning Applications for Behavioral Pattern Recognition

Beyond simple presence detection, machine learning enables the recognition of complex behavioral patterns that inform building operations. Network activity analysis can identify recurring meetings, collaborative work sessions, and other usage patterns that impact resource requirements. Deep learning algorithms process historical network data to discover behavioral trends that might escape human observation, such as seasonal variations in building usage or gradual shifts in work patterns. These recognized behaviors inform predictive models that anticipate future needs with increasing accuracy over time. Indoor positioning systems provide particularly valuable data for understanding movement patterns throughout buildings, enabling optimization of space allocation and resource distribution [7]. As these machine learning systems accumulate data over time, their predictive capabilities continue to improve, creating increasingly responsive and efficient building environments. The ability to recognize and anticipate occupant behaviors represents a fundamental advancement in building intelligence that transforms static infrastructure into dynamic, responsive environments.

5. Human-AI Collaboration in Network Policy Orchestration

The evolution of network management has progressed beyond automated configurations to a collaborative model where human expertise and artificial intelligence work in tandem. This collaborative approach enables network policies to align more closely with organizational objectives while maintaining the reliability and security required in enterprise environments. Human-AI collaboration represents a transformative approach to network orchestration that leverages the strengths of both human insight and machine intelligence.

5.1 Intent-Based Networking Frameworks

Intent-based networking (IBN) represents a paradigm shift in network management, focusing on business outcomes rather than technical configurations. These frameworks allow engineers to express desired network behaviors in business language, with AI systems translating these intentions into specific network configurations. IBN abstracts the complexity of network infrastructure, enabling communication between technical and non-technical stakeholders about network requirements. The implementation of intent-based networking involves multiple architectural components including intent translation, policy validation, automated implementation, and assurance monitoring [9]. These frameworks provide a foundation for human-AI collaboration by creating a common language for expressing network requirements and evaluating outcomes. The abstraction layer that IBN provides enables more strategic thinking about network policies, shifting focus from technical details to business objectives and allowing both human and artificial intelligence to contribute more effectively to network orchestration.

5.2 Translation of Business Objectives into Network Configurations

The translation of high-level business objectives into specific network configurations represents a critical function in human-AI collaboration. Network engineers articulate organizational requirements such as "optimize building energy usage during non-peak hours" or "prioritize emergency communications during critical events," while AI systems interpret these objectives and generate appropriate network policies. This translation process involves semantic understanding of business intent, mapping to technical capabilities, and generating compatible configurations across diverse network devices. The complexity of this translation would overwhelm purely manual processes, particularly in large enterprise environments with heterogeneous equipment. AI systems excel at managing this complexity while maintaining consistency across the network infrastructure. Federated multi-task learning approaches have demonstrated particular effectiveness for network management and orchestration tasks that require coordinated policies across distributed systems [10]. The collaboration between human intent expression and AI translation capabilities creates network policies that align technical implementations with organizational objectives more effectively than either could achieve independently.

5.3 Engineer Oversight and AI Refinement Processes

While AI systems handle much of the technical implementation, human engineers maintain critical oversight roles that ensure proper network functioning. Engineers review AI-generated configurations before deployment, validate that implementations align with intended outcomes, and intervene when necessary to address unique situations. This oversight relationship evolves over time as engineers gain confidence in AI recommendations and AI systems learn from engineer modifications. The supervisory role of network engineers shifts from direct configuration to policy guidance, exception handling, and performance evaluation. This transition represents a more strategic application of human expertise rather than a reduction in importance. Survey results on intent-based networking implementations have highlighted the critical importance of maintaining human oversight while leveraging AI capabilities for network management [9]. The complementary relationship between human judgment and machine efficiency creates network management processes that combine the best qualities of both, resulting in more robust and adaptable network infrastructures.

5.4 Development of Feedback Loops for Continuous Improvement

The effectiveness of human-AI collaboration in network policy orchestration depends on well-designed feedback mechanisms that enable continuous improvement. These feedback loops capture performance metrics, user experiences, and business outcomes to evaluate the success of implemented policies. AI systems analyze this feedback to refine their translation algorithms and recommendation engines, while engineers use the same information to adjust their intent specifications and oversight approaches. Federated learning techniques enable these improvement processes to operate across distributed network environments, aggregating insights without compromising security or privacy [10]. The multi-directional nature of these feedback processes—between humans and AI, between technical and business stakeholders, and across different network domains—creates a learning ecosystem that continuously enhances network policy effectiveness. As these feedback mechanisms mature, the collaborative relationship between human engineers and AI systems grows increasingly sophisticated, enabling more complex network policies and more precise alignment with business objectives. This evolution represents a fundamental advancement in network management that transcends both traditional manual configuration and simple automation to create truly intelligent network orchestration.

6. Conclusion

The integration of artificial intelligence into enterprise network management represents a transformative advancement for smart building ecosystems. As networks evolve from static infrastructure into dynamic, intelligent systems, the symbiotic relationship between AI capabilities and human expertise creates unprecedented opportunities for operational efficiency, security enhancement, and resource optimization. The progression from automated traffic classification to anomaly detection, environmental optimization, and intent-based orchestration demonstrates the multifaceted impact of AI across network functions. This technological evolution enables buildings to respond intelligently to changing conditions while maintaining optimal performance for diverse applications. Network engineers now operate at a more strategic level, defining intentions and validating outcomes rather than managing technical details, while AI systems handle increasingly complex implementation tasks with growing sophistication. The feedback mechanisms between human and machine intelligence foster continuous improvement cycles that enhance both technological capabilities and business outcomes. As smart buildings continue to increase in complexity and scale, the intelligence embedded within their network infrastructure will become an increasingly critical factor in operational success, occupant satisfaction, and sustainability performance. The future of enterprise networks lies not in artificial intelligence alone, but in the powerful collaborative relationship between human insight and machine intelligence that enables truly smart environments.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Andrew Crooks, et al., "Creating Smart Buildings and Cities," IEEE Pervasive Computing, Volume 16, Issue 2, March 31 2017. https://ieeexplore.ieee.org/document/7891102

[2] Aris Leivadeas; Matthias Falkner, "A Survey on Intent-Based Networking," IEEE Communications Surveys & Tutorials (Volume 25, Issue 1), October 20, 2022. https://ieeexplore.ieee.org/document/9925251/citations#citations

[3] Cheolhee Park, et al., "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," IEEE INTERNET OF THINGS JOURNAL, VOL. 10, NO. 3, 1 FEBRUARY, 2022. https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?arnumber=9908159

[4] Fahim Al Islam, et al., "BRURIIoT: A Dataset for Network Anomaly Detection in IIoT with an Enhanced Feature Engineering Approach," IEEE DataPort, March 6, 2025. https://ieee-dataport.org/documents/bruriiot-dataset-network-anomaly-detection-iiot-enhanced-feature-engineering-approach

[5] Francesc Wilhelmi, et al., "AI/ML-based Load Prediction in IEEE 802.11 Enterprise Networks," arXiv (Networking and Internet Architecture), October 11, 2023. https://arxiv.org/abs/2310.07467

[6] IEEE Computational Intelligence Society, "VERTICAL-AI for Energy – IEEE CAI 2025," IEEE CAI 2025, 2025. https://cai.ieee.org/2025/ai-for-energy/

[7] Ilka Miloucheva, et al., "Architecture for Dynamic Management of QoS Policies for Heterogeneous Internet Environments," IEEE Xplore, 08 October 2007. https://ieeexplore.ieee.org/document/4343416/citations#citations

[8] Md Shadab Mashuk, et al., "A Smart Phone-Based Multi-Floor Indoor Positioning System for Occupancy Detection," IEEE Xplore, 07 June 2018. https://ieeexplore.ieee.org/document/8373384

[9] Mira Rani Choudhury, et al., "Network Traffic Classification Using Supervised Learning Algorithms," IEEE Xplore, 03 April 2023. https://ieeexplore.ieee.org/abstract/document/10084931

[10] Rongpeng Li, et al., "Network AI Management & Orchestration: A Federated Multi-task Learning Case," IEEE Globecom Workshops, 24 January 2022. https://ieeexplore.ieee.org/document/9681969/authors#authors