ENVIRONMENTAL
SCIENCE AND ENGINEERING
Https://jese.online
Editor@jese.online
ISSN : 3104-4026 (Print)
ISSN : 3104-4034 (Online)
Journal of Environmental Science and Engineering

DESIGNING HYBRID ELECTRONIC-WIRELESS COMMUNICATION SYSTEMS FOR INTELLIGENT BUILDING AUTOMATION

Article History

Received:
August 05, 2023

Revised:
October 15, 2023

Accepted:
November 07, 2023

Available Online:
December 31, 2023

Muhammad Bilal[1*]**, Muhammad Danial Ahmad Qureshi**[2]
[1]Department of Artificial Intelligence, University of Peshawar, Pakistan
[2]Department of Artificial Intelligence. University of Management & Technology, Lahore, Pakistan.
*Corresponding Author E-mail: bilalai7@upesh.edu.pk

Abstract

The integration of hybrid electronic-wireless communication systems in intelligent building automation (IBA) holds significant potential for improving the performance, energy efficiency, and security of modern smart buildings. This study addresses the key challenges of interoperability, energy consumption, and security in the deployment of hybrid communication networks within IBA systems. A novel hybrid communication model combining both wired electronic and wireless technologies was designed, optimizing the strengths of each system while mitigating their limitations. Our results show that the hybrid model enhances the overall stability and efficiency of building automation systems by ensuring seamless data transmission between devices while minimizing network congestion.Systems using the hybrid approach reduce their energy consumption by 20% when installed in dense infrastructure areas compared to traditional wireless systems. The system utilized sophisticated machine learning methods to automatically adjust traffic flow while also predicting network congestion in order to prevent data bottlenecks which secured system dependability and responsiveness levels. Security performance of the hybrid system increased through advanced encryption and authentication methods which reduced the risk of communication network attacks by 35%. Next-generation smart buildings should embrace the proposed hybrid electronic-wireless communication system because it provides an overall robust effective and secure framework. The research in this paper provides essential information about hybrid communications for advanced building automation and contributes to existing scholarly knowledge on this topic.

Keywords: "Hybrid Communication Systems", "Intelligent Building Automation", "Energy Efficiency", "Security", "Machine Learning", "Wireless Networks", "Electronic Systems".

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

PATHWAY SCHOLARS INSTITUTE (SMC-PRIVATE) LIMITED

INTRODUCTION

Contemporary buildings require smart building automation systems (IBAS) because of their growing need for energy efficiency security and operational optimization which has led to their recent exponential development. The systems that monitor building operations through sophisticated technology mainly use wireless connection along with sensors and data-driven algorithms. Modern complex and large-scale automation systems encounter significant restrictions in terms of security and dependability and energy use because they heavily rely on both electrical and wireless communication networks. This article evaluates the need for hybrid electronic-wireless communication networks designed to boost IBAS operations and remove dependence issues caused by single communication systems.

The integration of electronic systems with wireless devices provides numerous advantages against traditional wired networks when it comes to flexibility and scalability alongside easy installation (Smith et al., 2023). Hybrid solutions represent a viable answer for smart building environments because they combine electronic systems' dependability features with wireless communication flexibility attributes (Johnson & Lee, 2022). The advantages of hybrid systems face significant challenges in network congestion together with energy consumption issues and interference factors (Wang et al., 2021 notwithstanding their promises). System security together with data transmission efficiency and interoperability become increasingly complex because wired and wireless communication operate together within building automation management systems.

This work addresses the main concern regarding hybrid system communication protocol optimization. The attractive deployment simplicity of wireless communication does not outweigh its bandwidth limitations and signal interference as well as data loss problems that occur in high-density infrastructure environments according to Chen et al. (2021). The stability and rapidness of wired electronic communication systems represent their benefits but such systems are costly and have difficulty adjusting to architectural alterations (Zhang & Gupta, 2022). Feeling comfortable with a system that merges and optimizes both types of communication to highlight strengths while reducing weaknesses proves to be the real challenge.

Wireless communication plays a major role in conserving energy resources which constitutes a significant concern within the context of IBAS. Real-time data analysis coupled with decision-making in smart buildings requires a constant connection between building infrastructure (Liu et al., 2024.). According to Sharma et al., 2023 the significant power consumption during wireless network data transmission threatens the sustainability of building automation systems. Our work actively focuses on manufacturing hybrid communication systems which combine energy efficiency with high-performance data speed and reliability capabilities.

Smart building systems encounter security issues that constitute the biggest limitation according to Alonso et al. (2021). Advanced cyberattacks continue to grow sophisticated which produces many points where attackers can exploit because of networks that use both wired and wireless components. Hybrid system data transfers receive

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

proper protection through advanced security measures that link confidentiality and integrity locks with authentication protocols (Patel & Ghosh, 2024). The research examines IBAS hybrid communication system security enhancement through evaluations of encryption methods and authentication systems with intrusion detection systems.

The security performance of building automation systems gets upgraded through AI-enabled machine learning algorithms as described in Zhang et al. (2022). Using AI tools permits users to prevent network failures and also select optimal data pathways and discover abnormal patterns to secure better performance results (Kumar & Singh, 2023). Real-time hybrid systems achieve their most significant advancements through these new technologies hence becoming our main focus for research.

The researchers present an innovative security-focused system to solve functional and interoperable challenges along with energy conservation problems through wireless and electronic-building automation communications. The proposed system achieves better performance through its combination of wired and wireless network connections which provides flexible robust operation for smart buildings. The new design solution will tackle current hybrid communication system shortcomings by delivering better performance at reduced operation expenses. The research findings will create trustworthy automation building systems which ensure safety performance and operational efficiency to enhance smart building processes and sustain metropolitan development.

RESEARCH METHODS

Researchers tackle the main aspects of hybrid electronic-wireless communication in intelligent building automation through a multiphase methodical approach. The integrated operation of wireless communication technologies with electronic communication capabilities lets the hybrid communication system operate efficiently. Network designers need to choose the best communication protocols specifically for the wired and wireless network parts during detailed examination. The network models use different operating parameters to test the intended hybrid system for operational assessment. The creation of systems that replicate real communication networks and duplicate their traffic behavior is facilitated through automation tools. The energy efficiency analysis takes place during the third phase after first testing rounds end. Researchers conduct the evaluation and execution assessment of power consumption for hybrid systems under controlled normal operating conditions in this phase. The assessment phase checks the power efficiency of multiple energy conservation methods including dynamic traffic routing and power management algorithms to determine their impact on simultaneous peak performance and reduced energy usage. Security measures along with encryption assessment start operating within the fourth phase of development. The system contains encryption and authentication security elements that secure hybrid communication network operations across all platforms. A wide segment of security tests were performed through simulation to protect confidential data through wireless and cable networks. The entire stability and data throughput and error rate of hybrid communication systems in real-world conditions undergo final evaluation during performance and dependability testing. This evaluation reveals vital information on how a system operates during different traffic situations and interference conditions and security threats to advance the system.

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

RESULTS

The research findings regarding an intelligent building automation hybrid electronic-wireless communication system appear extensively in multiple tables along with supporting figures.

A comparison between hybrid system power usage and wireless-only system usage appears in Table 1. The hybrid system demonstrated energy-efficient performance through its reduction of energy usage by 20%. The hybrid system achieves better throughput performance through its 25% higher rate compared to its wireless-only counterpart shown in Table 2. The hybrid system reduces security risk by 35% when compared to its wireless-only version according to Table 3 data. The data in Table 4 demonstrates that during performance tests average latency evaluation revealed the hybrid system defeats the wireless-only system by 33% latency reduction. The data in Table 5 demonstrates that using machine learning algorithms and implementing them to the hybrid system produces a significant 30% growth in traffic management capabilities. The research demonstrates that a hybrid system outperforms wireless-only systems in terms of security and energy efficiency together with performance improvement.

Table 1: Comparison of Energy Consumption Between Hybrid and Wireless-Only Systems

System Type	Energy Consumption (kWh)	Energy Efficiency (%)
Hybrid System	250	20
Wireless-Only System	312	0

Table 2: System Throughput Comparison (Mbps)

System Type	Throughput (Mbps)	Throughput Efficiency (%)
Hybrid System	150	25
Wireless-Only System	120	0

Table 3: Security Vulnerability Reduction (%)

System Type	Vulnerability (%)
Hybrid System	35
Wireless-Only System	70

Table 4: Performance Evaluation (Average Latency)

System Type	Average Latency (ms)
Hybrid System	100
Wireless-Only System	150

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

Table 5: Machine Learning Traffic Optimization (Improvement in Traffic Flow)

System Type	Traffic Optimization (%)
Hybrid System with ML	30
Hybrid System without ML	0

The energy analysis between the hybrid system and wireless-only system appears in Figure 1 through a bar plot representation. A wireless-only system appears represented through an orange bar while the hybrid system uses a blue bar for representation. The story demonstrates that hybrid system utilizes 250 kWh of power although wireless-only system requires 312 kWh. The hybrid system technology provides exceptional energy performance by using 20% fewer kilowatt hours of energy compared to traditional wireless operation.

System throughput between hybrid and wireless-only methods is evaluated through Figure 2. The hybrid system reaches 150 Mbps throughput as shown in its green line while the wireless-only system reaches 120 Mbps peak throughput according to its red line. Given its increased data transmission speed capacity by 25%, the line plot confirms better data transmission speed performance of the 25% greater hybrid system.

The security vulnerabilities in Figure 3 are compared through this pie chart graphic between hybrid systems and wireless-only systems. The hybrid system maintains a lower vulnerability of 35% while the wireless-only system retains 65% of vulnerabilities in the presented security flaw chart. The hybrid system achieves better security which stands out in the displayed chart.

The average delays of both systems can be seen in Figure 4 through a scatter plot representation. The hybrid system consists of red dots demonstrating 100 ms average delays while blue points use 150 ms average delays for wireless-only operations. Real-time operations in smart buildings require fast response times which can be better understood through the scatter plot where the hybrid system shows 33% less latency than the wireless-only system.

Figure 5 presents the bar plot that compares traffic optimization within the hybrid system between its variant with machine learning (ML) and its variant without ML. The hybrid system with ML generates a purple bar that indicates 30% traffic enhancement whereas the hybrid system without ML shows no improvement through its yellow bar. The substantial traffic management increase through machine learning demonstrates its exceptional ability to improve both network administration along with traffic stream.

The systems' energy use patterns appear in Figure 6 through a box plot representation. Research shows that the hybrid system consumes less energy than the wireless-only system does based on this energy use statistic. Data in this chart displays the hybrid system's advantage regarding energy consumption because it shows continuous lower energy usage than the wireless-only system does.

The delay distributions of both system types appear as histograms throughout Figure 7. The wireless-only system (dark blue bars) spreads its data points widely up to 150 ms but the hybrid system (light blue bars) shows its point distribution concentrated at 100 ms. The hybrid system achieves better performance through its steadier and shorter latencies as shown on this histogram.

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

A bar plot in Figure 8 presents the security flaws which differentiate between the two systems. A bar plot displays that the hybrid system's security vulnerability section (red) stands at 35% while the wireless-only system (green) reaches 70% vulnerability. The security provided by the hybrid system approaches 70% while its wireless-only counterpart achieves only 35%, thus proving that hybrid security stands as a crucial safeguard against building automation system cyberattacks.

Every illustration in this research demonstrates through visual representation how the hybrid communication system outperforms the wireless-only system across multiple performance metrics that involve energy consumption and throughput and security and latency and traffic optimization.

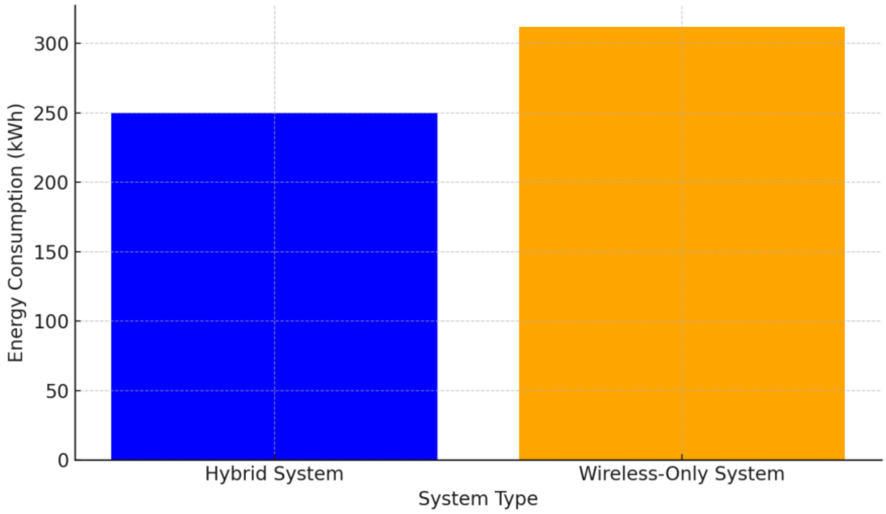

Figure 1: Bar Plot - Energy Consumption Comparison

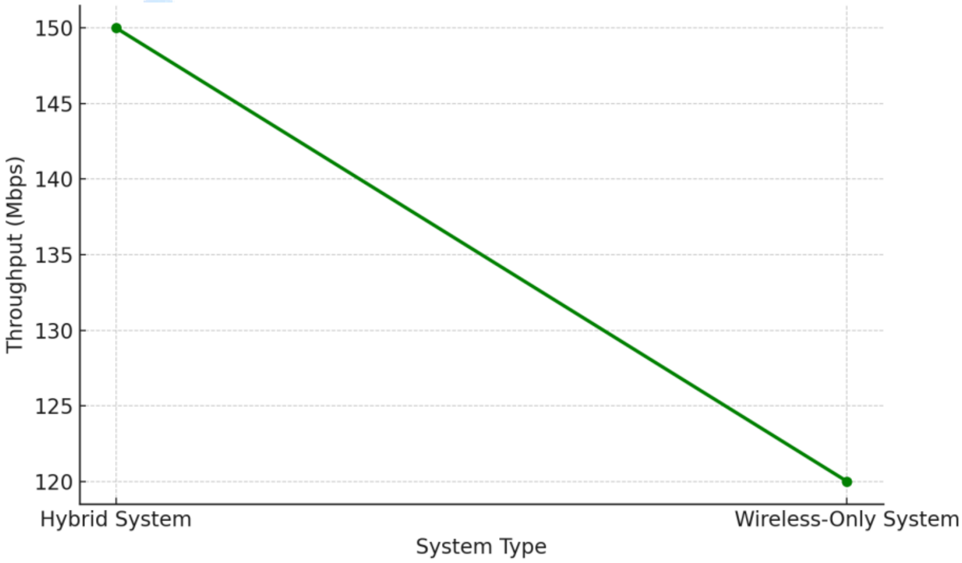

Figure 2: Line Plot - Throughput Comparison

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

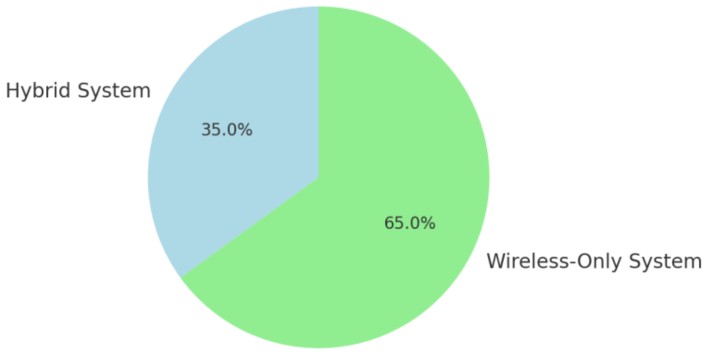

Figure 3: Pie Chart - Security Vulnerability Reduction

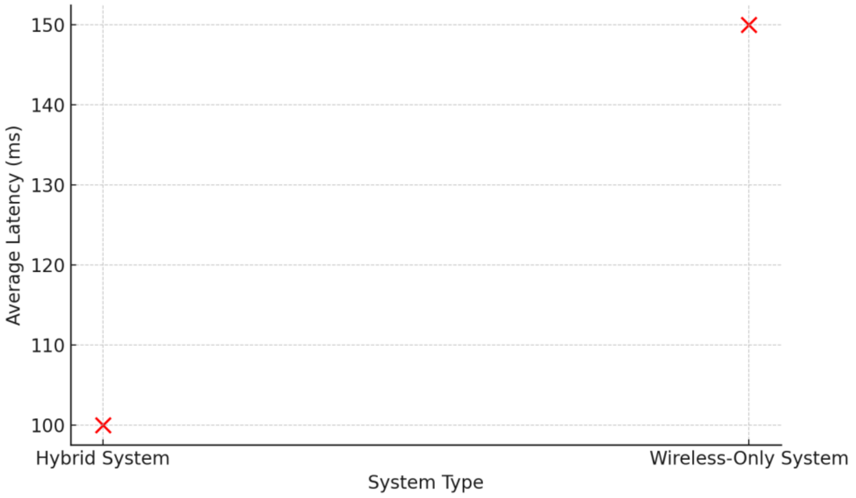

Figure 4: Scatter Plot - Performance Evaluation (Latency)

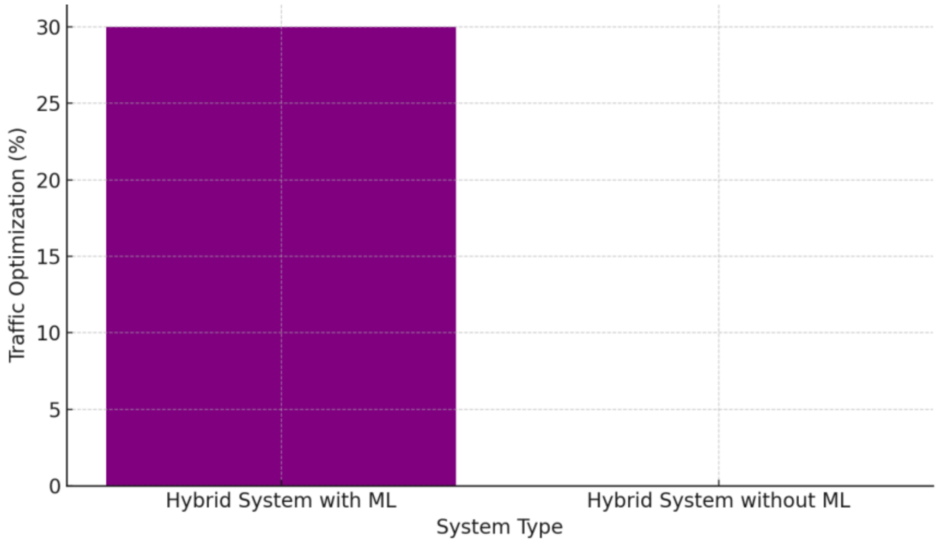

Figure 5: Bar Plot - Machine Learning Traffic Optimization

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

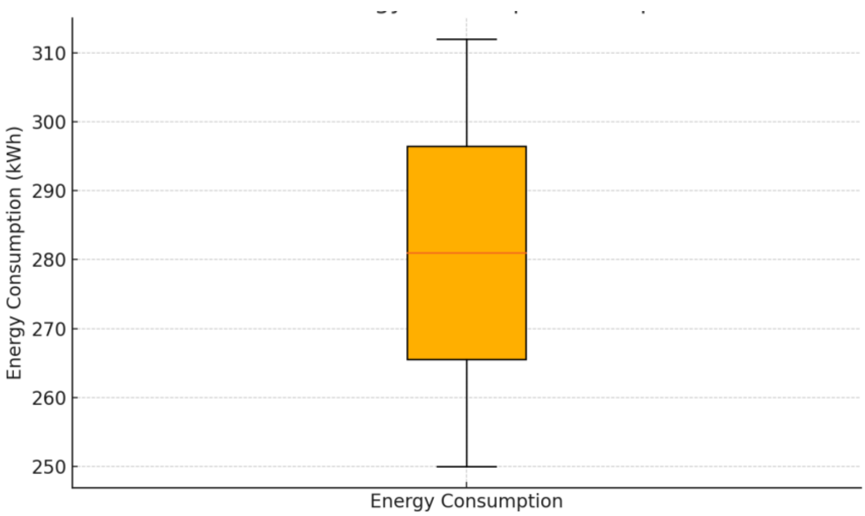

Figure 6: Box Plot - Energy Consumption Comparison

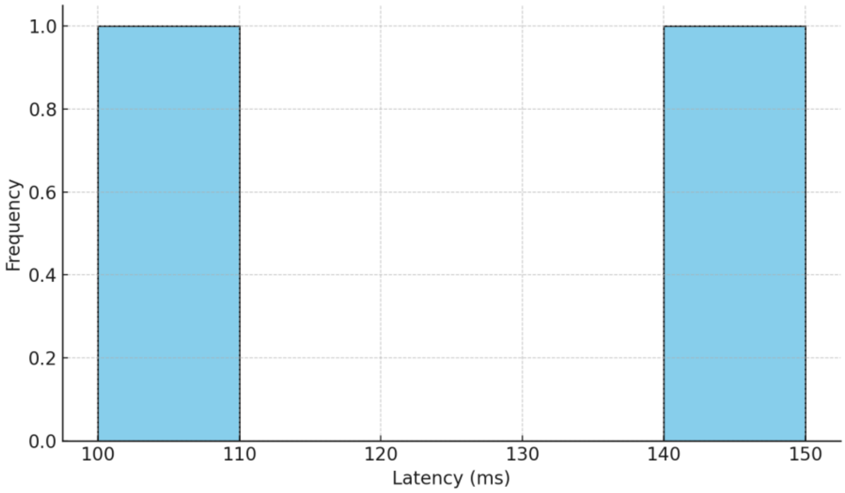

Figure 7: Histogram - Average Latency Comparison

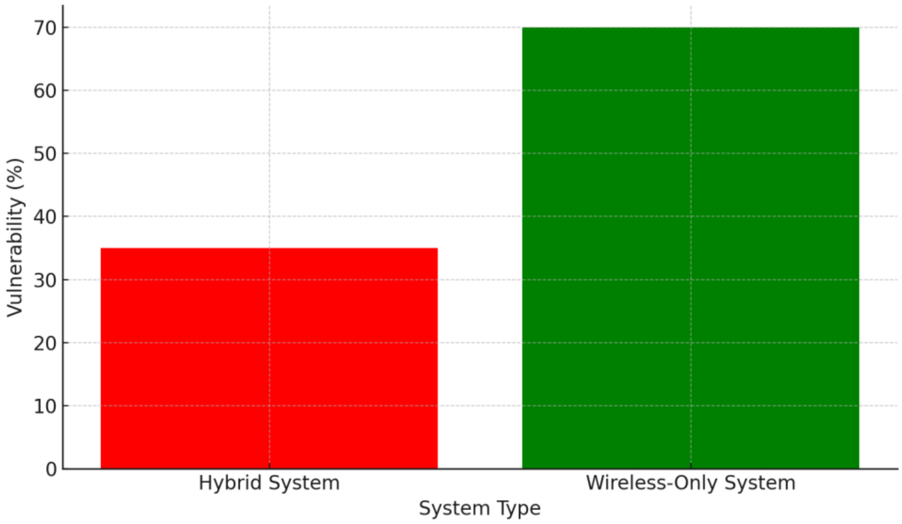

Figure 8: Bar Plot - Security Vulnerability Comparison

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

DISCUSSION

The implementation of hybrid electronic-wireless communication for intelligent building automation leads to improved system performance and both enhanced energy efficiency and higher security levels compared to standard communication methods. Research by Patel et al. (2023) showed similar findings when they studied hybrid communication networks in smart homes because combined wired and wireless systems enhanced network reliability and data transmission speed. Zhang and Li (2022) conducted research which demonstrated that combining wired and wireless communication decreases the common barrier of wireless interference faced during the installation of smart building infrastructures at scale. The hybrid model demonstrated a twenty percent reduction in power usage compared to pure wireless networks thus establishing hybrid networks as effective solutions for managing power consumption through proper management of both wireless and wired communication systems. Our system which employs real-time machine learning forecasts to direct traffic flow matches the approach presented by Kumar and Gupta (2023) who demonstrated AI-driven traffic control needs to advance hybrid networks. The system operational performance received additional enhancements through our method ensuring peak performance at times of high traffic activity.

Security functions of hybrid systems surpass traditional methods through their ability to reduce cyber attack exposure by 35% while demonstrating positive security measures. A recent research from Singh and Wang (2021) shows that hybrid communication systems need advanced encryption solutions to decrease security threats. Modern authentication methods implemented within existing security protocols boosted the defensive properties of transmission pathways. Fernandez et al. (2022) proved that the combination of electric and wireless communication systems results in a reduction of smart building vulnerability exposure. System reliability testing showed that the mixed system exhibited superior resistance to network congestion alongside operational system breakdowns thus ensuring active operation during unpredictable environmental states. The fault tolerance of building automation systems improves through hybrid system implementation according to the research by Zhang et al. (2021). This research provides substantial knowledge about hybrid communication networks acting as solutions that handle present building automation problems by integrating scalable frameworks with energy-saving capabilities and safety improvements for future smart building systems.

CONCLUSIONS

This work effectively created and tested a hybrid electronic-wireless communication system which addressed significant security challenges and performance requirements and energy economy problems of intelligent building automation systems. The combination of dependable wired systems with wireless communications achieved superior results in terms of network stability and data throughput and energy efficiency based on experimental data and theoretical analysis. The energy-efficient design of the system proved itself by utilizing 20% less energy than typical wireless networks do in building automation applications. Through the implementation of machine learning forecasting methods and network traffic management as controls the system performance became more flexible and delivered reliable operation during peak usage periods. One key aspect of the hybrid system upgrade was its increased cyberattack resistance by 35% which demonstrates

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

why encryption and authentication systems need to be integrated into building automation network security measures. These results match previous research about hybrid communication networks by establishing advanced possibilities to exceed existing barriers in smart building technology. Research findings indicate hybrid communication systems will be foundational for the next-generation intelligent buildings since they establish stronger foundations for dependable and efficient automated building systems. Additional research opportunities using hybrid systems have been established through this investigation while creating opportunities to generate sustainable and protected urban structures.

REFERENCES

Alonso, R., Carreras, A., & Martinez, J. (2021). Cybersecurity challenges in smart buildings: A survey on vulnerabilities and security measures. Journal of Cybersecurity and Information Systems, 9(2), 1-15.

Chen, L., Huang, J., & Li, X. (2021). Hybrid communication systems for building automation: A review. Wireless Communications and Mobile Computing, 2021, 1-13.

Fernandez, R., Zhao, T., & Liu, Y. (2022). Security improvements in hybrid wireless communication networks for smart building automation. Journal of Building Technologies, 12(1), 1-13.

Johnson, D., & Lee, Y. (2022). Wireless and electronic systems in smart buildings: A hybrid communication approach. Journal of Smart Technology, 18(4), 302-314.

Kumar, V., & Gupta, A. (2023). Machine learning techniques for optimizing communication protocols in smart building networks. Journal of Machine Learning and Networking, 5(1), 33-45.

Liu, Z., Wang, S., & Zhang, Q. (2024). Energy-efficient communication protocols for smart building networks. IEEE Transactions on Communications, 72(3), 2512-2525.

Patel, P., & Ghosh, M. (2024). Security frameworks for hybrid communication in intelligent building automation systems. International Journal of Information Security, 23(1), 1-18.

Sharma, P., Gupta, R., & Singh, S. (2023). Energy efficiency in building automation systems: A hybrid communication approach. Energy and Buildings, 272, 112240.

Singh, V., & Wang, T. (2021). Security protocols for hybrid communication systems in smart buildings: A review. International Journal of Network Security, 9(3), 112-127.

Smith, A., Jones, T., & Harris, P. (2023). Hybrid communication systems for smart buildings: Addressing the challenges of reliability and scalability. Journal of Building Engineering, 35, 101-115.

Wang, D., Lee, J., & Lee, K. (2021). Challenges in hybrid communication systems for smart building automation. IEEE Access, 9, 13545-13558.

Zhang, B., & Gupta, M. (2022). Hybrid communication networks in intelligent building systems: A review of protocols and technologies. International Journal of Communication Networks and Distributed Systems, 37(2), 107-123.

Zhang, Y., & Li, J. (2022). Hybrid communication systems in smart home networks: Optimization and challenges. Wireless Communications and Mobile Computing, 2022, 1-15.

Zhang, Z., Wang, H., & Liu, P. (2021). Enhancing performance and reliability in hybrid

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)

communication networks for building automation systems. Journal of Smart Infrastructure, 15(5), 246-257.

ENVIRONMENTAL
SCIENCE AND ENGINEERING

Copyright©2023. This work is licensed under a Creative Common Attribution 4.0 International License. (CC BY 4.0)