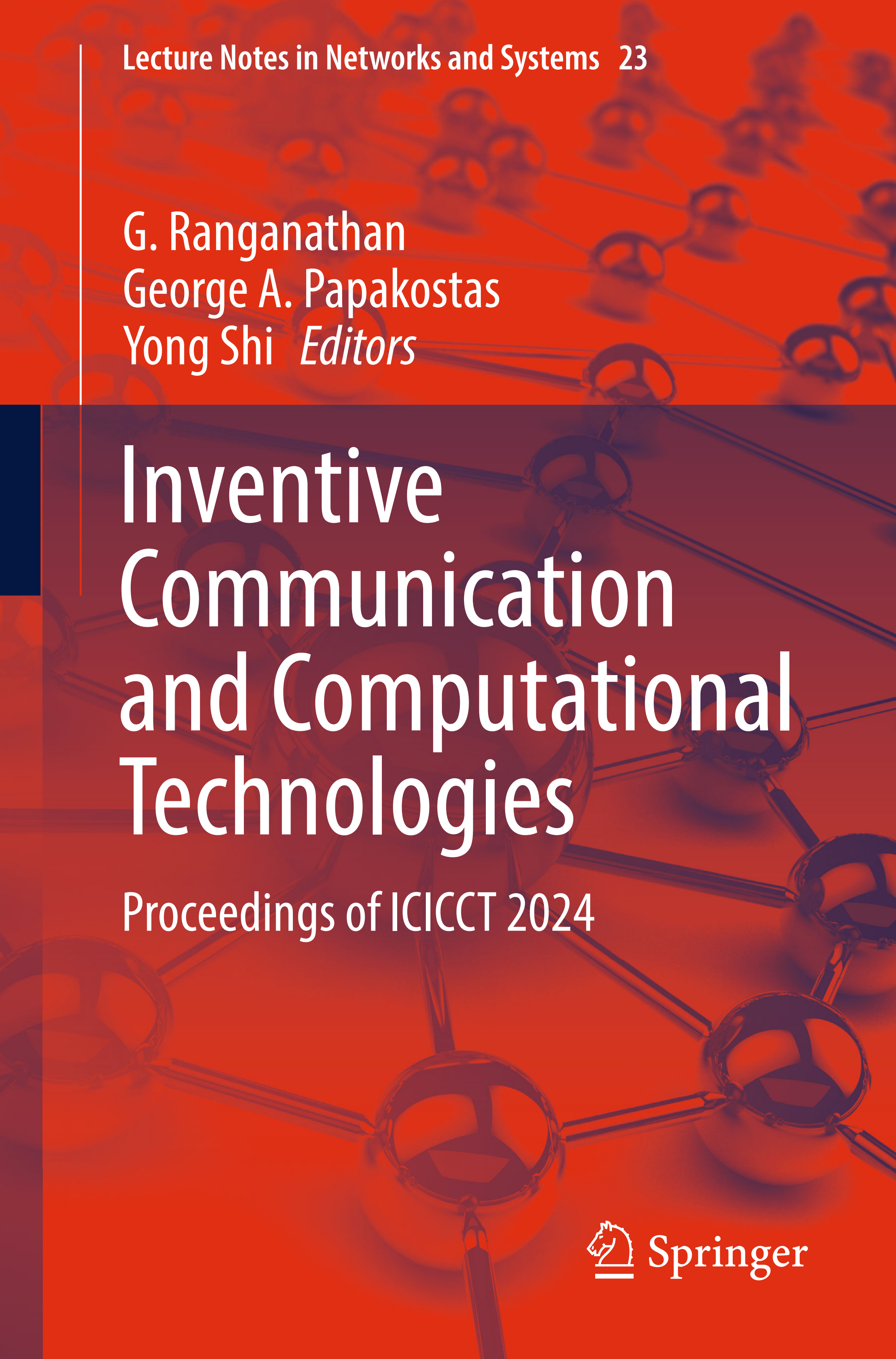
Lecture Notes in Networks and Systems 23



G. Ranganathan
George A. Papakostas
Yong Shi *Editors*

Inventive Communication and Computational Technologies

Proceedings of ICICCT 2024

Springer

Lecture Notes in Networks and Systems

Volume 23

G. Ranganathan · George A. Papakostas · Yong Shi
Editors

Inventive Communication and Computational Technologies

Proceedings of ICICCT 2024

Springer

Editors
G. Ranganathan
Sree Sakthi Engineering College
Coimbatore, Tamil Nadu, India

Yong Shi
Department of Computer Science
Kennesaw State University
Kennesaw, GA, USA

George A. Papakostas
Department of Computer Science
(HUMAIN-Lab)
International Hellenic University
St. Loukas, Greece

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-97-7709-9 ISBN 978-981-97-7710-5 (eBook)
https://doi.org/10.1007/978-981-97-7710-5

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

With a great deal of dedication, 8th ICICCT 2024 is dedicated to all the authors, great scientists, academicians, young researchers, conference delegates, and students, who have research expertise on ICT technologies from all over the world. Nevertheless, this proceedings is dedicated to cover a wide spectrum of themes related to intelligent computing and communication innovations and developments.

Preface

The 2024 International Conference on Inventive Communication and Computational Technologies (ICICCT 2024) took place in Coimbatore, India, from June 14–15, 2024. ICICCT 2024 aimed to explore recent advancements and emerging trends in communication and computational technologies, fostering knowledge sharing and networking among researchers and industry experts.

The conference encompassed a wide array of topics including computing networks, security, blockchain, image processing, computer vision, recommendation systems, fault diagnosis, deep learning, and neural networks. From a total of 342 submissions received from universities and industries worldwide, 75 papers were selected for presentation based on their quality and relevance following rigorous peer review by 2–4 expert referees.

We extend our sincere appreciation to all authors for their valuable contributions to this volume. Our gratitude also goes to the referees for their insightful comments that helped enhance the quality of the selected papers. Special thanks are due to the organizing committee for their diligent efforts in ensuring the success of ICICCT 2024. Lastly, we acknowledge Springer publications for their role in producing this compilation.

Coimbatore, India

Dr. G. Ranganathan
Conference Chair
ICICCT 2024

Contents

Ensuring Data Transmission Security Through Wi-Fi 6, ZigBee, and Li-Fi Technologies in Smart City Integration

Islambek Rustambekov, Saidakhror Gulyamov, Naeem Allahrakha, Islombek Abdikhakimov, San'at Ergashev, Bobur Saidov, and Ekaterina Kan

Abstract This comprehensive research study examines the cybersecurity aspects of integrating Wi-Fi 6, ZigBee, and Li-Fi technologies within smart city ecosystems. The paper analyzes the security risks, threats, and necessary mitigation measures to ensure the confidentiality, integrity, and availability of transmitted data. It explores data protection methods in Wi-Fi 6 networks, security of ZigBee automation systems, and the unique security advantages of Li-Fi technology. The study also proposes the integration of security systems into a unified smart city management platform leveraging blockchain and AI, enhancing overall resilience. The findings provide practical implications for smart city stakeholders and contribute to the advancement of secure and resilient urban infrastructure.

Keywords Smart city · Cybersecurity · Wi-Fi 6 · ZigBee · Li-Fi · Blockchain · AI

1 Introduction

1.1 Relevance and Significance of the Research Topic

The proliferation of smart city initiatives worldwide has underscored the critical importance of secure data transmission across various interconnected technologies. As cities strive to enhance urban efficiency, sustainability, and citizen engagement, the integration of wireless communication protocols such as Wi-Fi 6, ZigBee, and Li-Fi has become pivotal. These cutting-edge technologies enable the seamless exchange of data essential for the smooth functioning of smart city applications, ranging from traffic management and energy distribution to public safety and healthcare [1]. However, the inherent security vulnerabilities associated with these wireless

I. Rustambekov (✉) · S. Gulyamov · N. Allahrakha · I. Abdikhakimov · S. Ergashev · B. Saidov · E. Kan
Tashkent State University of Law, Tashkent, Uzbekistan
e-mail: irustambekov2024tsult@mail.ru

G. Ranganathan et al. (eds.), *Inventive Communication and Computational Technologies*, Lecture Notes in Networks and Systems 23,
https://doi.org/10.1007/978-981-97-7710-5_73

technologies pose significant challenges in ensuring the confidentiality, integrity, and availability of the transmitted information.

This research paper aims to provide a comprehensive analysis of the cybersecurity aspects involved in the integration of Wi-Fi 6, ZigBee, and Li-Fi technologies within smart city ecosystems. By examining the key security risks, threats, and necessary mitigation measures, the study will contribute to the development of robust data protection strategies, ultimately strengthening the overall resilience of smart city infrastructure [2].

2 Methodology

2.1 Data Collection and Synthesis

The research methodology employed in this study combines a thorough review of existing literature, analysis of industry reports, and expert consultations to synthesize a comprehensive understanding of the security considerations surrounding the integration of Wi-Fi 6, ZigBee, and Li-Fi technologies in smart cities. The data collection process involved the following steps:

1. Systematic literature review: A comprehensive search of academic databases, such as IEEE Xplore, Scopus, and Web of Science, was conducted to identify the latest research, case studies, and industry best practices related to the cybersecurity aspects of smart city technologies.
2. Industry report analysis: Relevant industry reports and white papers from leading technology organizations, standards bodies, and research institutions were examined to gain insights into the current state of security challenges and emerging trends in the smart city domain.
3. Expert consultations: Interviews and focus group discussions were held with subject matter experts, including cybersecurity professionals, smart city practitioners, and technology leaders, to gather first-hand knowledge and perspectives on the security implications of integrating Wi-Fi 6, ZigBee, and Li-Fi in smart city environments.

The data collected through these methods was systematically analyzed and synthesized to develop a comprehensive understanding of the security landscape, identify key risks and threats, and formulate strategies to address the challenges.

2.2 Comparative and Inductive Approach

The research framework employed in this study follows a comparative and inductive approach to derive meaningful insights and actionable recommendations. This methodological approach involves the following steps:

1. Comparative analysis: The security features, vulnerabilities, and best practices associated with Wi-Fi 6, ZigBee, and Li-Fi technologies were analyzed and compared to identify the unique security considerations and interdependencies within a smart city context.
2. Inductive reasoning: By examining the security implications of integrating these technologies, the research team inductively identified the critical security requirements, emerging threats, and necessary mitigation strategies to ensure the confidentiality, integrity, and availability of data transmitted in smart city systems.
3. Holistic integration: The research findings were then synthesized to develop a holistic approach to securing data transmission across the smart city ecosystem, leveraging the strengths, and addressing the weaknesses of the individual wireless technologies.

This comparative and inductive approach enabled the research team to derive comprehensive insights and formulate practical recommendations for enhancing the cybersecurity posture of smart city infrastructure through the seamless integration of Wi-Fi 6, ZigBee, and Li-Fi technologies.

3 Results

3.1 Description of Key Cybersecurity Aspects in the Interaction of Wi-Fi 6, ZigBee, and Li-Fi Technologies in Smart Cities

The integration of Wi-Fi 6, ZigBee, and Li-Fi technologies within smart city ecosystems introduces a complex web of cybersecurity considerations that must be addressed to ensure the protection of sensitive data and the overall resilience of the system. Each of these wireless technologies possesses unique security characteristics, vulnerabilities, and mitigation strategies that must be carefully examined and harmonized to create a robust and secure smart city infrastructure.

Wi-Fi 6, the latest iteration of the Wi-Fi standard, offers enhanced security features such as improved encryption, authentication, and device management capabilities [3]. However, the sheer scale and interconnectivity of smart city applications make Wi-Fi 6 networks vulnerable to various threats, including network congestion, unauthorized access, and advanced persistent threats. Addressing these challenges requires a multilayered approach, incorporating robust access control mechanisms, intrusion detection and prevention systems, and proactive monitoring and response strategies.

ZigBee, a widely adopted wireless protocol for smart city automation and control systems, presents its own set of security concerns. The resource-constrained nature of ZigBee devices and the potential for large-scale deployments in urban environments heighten the risk of exploitation, such as device hijacking, data tampering, and denial-of-service attacks [4]. Securing ZigBee networks demands a comprehensive approach, including the implementation of strong cryptographic measures, device authentication, and intrusion detection systems specifically tailored for the unique characteristics of the ZigBee protocol.

Li-Fi, an emerging light-based communication technology, offers inherent security advantages due to its reliance on line-of-sight transmission and the confined nature of its signal propagation [5]. However, the integration of Li-Fi within smart city infrastructure introduces new security considerations, such as the potential for eavesdropping, jamming, and the need for secure handover between Li-Fi and other wireless technologies. Ensuring the confidentiality and integrity of Li-Fi-based data transmission requires the development of robust key management systems, advanced authentication mechanisms, and seamless integration with the broader smart city security framework.

To address the complex security challenges arising from the integration of these wireless technologies, a holistic and collaborative approach is essential. This includes the development of comprehensive security policies, the implementation of advanced security controls, the adoption of secure system design principles, and the continuous monitoring and adaptation of security measures to address evolving threats. By addressing the unique security requirements of Wi-Fi 6, ZigBee, and Li-Fi, smart city stakeholders can establish a secure and resilient data transmission infrastructure, ultimately safeguarding the privacy, integrity, and availability of vital information for the effective operation and management of smart city services.

3.2 Data Protection Methods in Wi-Fi 6 Networks for Smart Cities, Including New Standard Capabilities for Enhancing Security

The deployment of Wi-Fi 6 technology within smart city environments presents both opportunities and challenges in terms of data protection. The Wi-Fi 6 standard has introduced several security enhancements that aim to address the evolving security landscape and the unique requirements of smart city applications.

One of the key security improvements in Wi-Fi 6 is the implementation of the Enhanced Open (EOP) feature, which provides automatic encryption for open Wi-Fi networks without the need for user intervention [6]. This feature helps to mitigate the risks associated with legacy open Wi-Fi networks, which are susceptible to eavesdropping and man-in-the-middle attacks. By default, Wi-Fi 6 devices establish a secure connection, ensuring the confidentiality of data transmitted over the wireless network.

Furthermore, Wi-Fi 6 introduces stronger encryption algorithms, such as the implementation of the WPA3 security protocol, which offers enhanced protection against offline password-guessing attacks and provides forward secrecy for encrypted communications [7]. This improved encryption mechanism is particularly crucial in smart city environments, where a vast number of connected devices and users require secure access to various services and applications.

The Wi-Fi 6 standard also includes advanced authentication and access control features, such as the adoption of the Opportunistic Wireless Encryption (OWE) protocol and the implementation of the Wi-Fi CERTIFIED Enhanced Open certification program [8]. These mechanisms enable seamless and secure onboarding of devices, ensuring that only authorized entities can access the Wi-Fi 6 network and mitigating the risks of unauthorized access and device impersonation.

Additionally, Wi-Fi 6 introduces the concept of Target Wake Time (TWT), which allows for more efficient power management and reduced device activity, thereby minimizing the attack surface and the potential for resource exhaustion attacks [9]. This feature is particularly beneficial in smart city scenarios, where numerous battery-powered IoT devices are deployed, as it enhances the overall security posture by reducing the vulnerability of these devices to malicious activities.

To further strengthen the security of Wi-Fi 6 networks in smart city environments, it is crucial to implement a comprehensive security strategy that encompasses the following elements:

1. Strict access control and authentication mechanisms: Leveraging the advanced authentication features of Wi-Fi 6, such as WPA3 and OWE, to ensure only authorized devices and users can access the network.
2. Continuous monitoring and threat detection: Deploying robust intrusion detection and prevention systems to identify and mitigate security threats in real-time, including network anomalies, unauthorized access attempts, and suspicious activities.
3. Secure device management and firmware updates: Implementing centralized device management platforms to ensure timely firmware updates and security patches, reducing the attack surface and vulnerabilities within the smart city infrastructure.
4. Security awareness and training: Educating smart city stakeholders, including citizens, on the importance of cybersecurity best practices and the secure use of Wi-Fi 6 networks to foster a culture of security awareness.

By embracing the security enhancements offered by the Wi-Fi 6 standard and implementing a holistic security strategy, smart city administrators can effectively protect the confidentiality, integrity, and availability of data transmitted over the Wi-Fi 6 network, ensuring the overall resilience and trustworthiness of the smart city ecosystem.

3.3 Ensuring the Security of ZigBee Automation Networks in Urban Infrastructure

The widespread adoption of ZigBee technology in smart city automation and control systems presents unique security challenges that must be addressed to ensure the protection of critical urban infrastructure. ZigBee, a low-power wireless protocol widely used in building automation, energy management, and smart metering applications, inherently faces security risks due to its resource-constrained nature and the potential for large-scale deployments in complex smart city environments.

To safeguard ZigBee-based systems in smart cities, a multilayered security approach is essential, encompassing the following key elements:

Cryptographic Protection: The ZigBee specification includes provisions for encryption and authentication mechanisms, such as the use of Advanced Encryption Standard (AES) with 128-bit keys [10]. However, the effective implementation and management of these cryptographic controls are crucial to prevent unauthorized access, data tampering, and eavesdropping. Smart city administrators must ensure the use of strong key generation, distribution, and rotation processes to maintain the confidentiality and integrity of ZigBee-based communications.

Node Authentication: The authentication of ZigBee devices is paramount to mitigate the risks of unauthorized access and device impersonation. This can be achieved through the implementation of robust certificate-based authentication or pre-shared key mechanisms, ensuring that only legitimate and trusted nodes are allowed to join the ZigBee network and participate in data exchange [11]. Periodic re-authentication and the use of secure commissioning procedures further enhance the overall security posture.

Intrusion Detection and Prevention: Given the potential for large-scale ZigBee deployments in smart city environments, the implementation of intrusion detection and prevention systems (IDPS) is crucial. These systems can monitor ZigBee network traffic, identify anomalous activities, and promptly detect and mitigate security threats, such as denial-of-service attacks, network flooding, and unauthorized access attempts [12]. By integrating IDPS capabilities, smart city administrators can enhance the resilience of their ZigBee-based automation systems.

Additionally, the security of ZigBee-enabled smart city infrastructure can be further strengthened through the following measures:

1. Secure firmware updates: Ensuring the availability of timely security patches and firmware updates to address known vulnerabilities and mitigate emerging threats.
2. Secure network segmentation: Partitioning the ZigBee network into logical segments or domains to limit the impact of security breaches and contain the spread of potential attacks.
3. Secure key management: Implementing robust key management practices, including the use of hardware security modules (HSMs) or trusted platform modules (TPMs) to securely store and manage cryptographic keys.

4. Secure commissioning and decommissioning: Establishing secure procedures for the onboarding and removal of ZigBee devices to prevent unauthorized access and ensure the overall integrity of the smart city infrastructure.

By adopting these comprehensive security measures, smart city administrators can effectively safeguard their ZigBee-based automation systems, ensuring the confidentiality, integrity, and availability of critical data transmitted across the urban infrastructure.

3.4 Ensuring Data Transmission Security Through Li-Fi Technology, Leveraging Its Unique Characteristics for Confidentiality

The emergence of Li-Fi, a wireless communication technology that utilizes visible light for data transmission, presents new opportunities and challenges in the context of smart city security. The inherent characteristics of Li-Fi, such as its reliance on line-of-sight transmission and the confined nature of its signal propagation, offer inherent security advantages that can be leveraged to enhance the confidentiality of data transmission within smart city environments.

One of the key security benefits of Li-Fi is the reduced risk of eavesdropping compared to traditional radio frequency (RF)-based wireless technologies. The confined nature of the light-based signal transmission in Li-Fi makes it more challenging for unauthorized parties to intercept the data, as the signal cannot easily penetrate walls or obstacles [5]. This physical layer security feature enhances the confidentiality of Li-Fi-based communications, reducing the risk of sensitive information being accessed by malicious actors.

Furthermore, the line-of-sight requirement of Li-Fi transmission introduces an additional layer of security, as it limits the access points from which an attacker can potentially intercept the data. This characteristic makes it more difficult for adversaries to gain unauthorized access to the Li-Fi network, as they would need to be physically present within the line of sight of the transmitting and receiving devices [13]. To further strengthen the security of Li-Fi-based data transmission in smart city environments, the following measures can be implemented:

1. Secure handover and session management: Ensuring seamless and secure handover between Li-Fi and other wireless technologies, such as Wi-Fi or cellular networks, to prevent session hijacking or man-in-the-middle attacks during transitions.
2. Advanced authentication and access control: Implementing robust authentication mechanisms, such as biometric authentication or device-based certificates, to ensure only authorized entities can access the Li-Fi network and participate in data exchange.

3. Secure key management: Developing secure key management protocols to establish and distribute encryption keys for Li-Fi-based communications, ensuring the confidentiality of the transmitted data.
4. Secure network design and zoning: Adopting a zonal approach to Li-Fi network design, where sensitive data is transmitted within secured zones with enhanced physical and logical access controls, while less sensitive data can be transmitted in open Li-Fi zones.
5. Intrusion detection and response: Deploying intrusion detection and prevention systems specifically tailored for Li-Fi networks, capable of identifying and mitigating threats such as jamming attacks or unauthorized access attempts.

By leveraging the inherent security advantages of Li-Fi technology and implementing a comprehensive security strategy, smart city administrators can enhance the confidentiality of data transmission and protect critical information assets within the smart city ecosystem. The integration of Li-Fi-based communication, in conjunction with other wireless technologies like Wi-Fi 6 and ZigBee, can contribute to the overall security and resilience of the smart city infrastructure.

3.5 Integration of Security Systems into a Unified Smart City Management Platform Leveraging Blockchain and AI Technologies

The effective integration of security systems across the various wireless technologies employed in smart cities requires a holistic and unified approach to data management and decision-making. The development of a centralized smart city management platform that seamlessly incorporates the security measures for Wi-Fi 6, ZigBee, and Li-Fi can significantly enhance the overall cybersecurity posture of the urban infrastructure.

The integration of such a platform can leverage the capabilities of emerging technologies, such as blockchain and artificial intelligence (AI), to strengthen the security and resilience of the smart city ecosystem. Blockchain technology can be utilized to establish a secure and decentralized data management system, enabling the immutable recording of security events, access logs, and device configurations across the various wireless networks [14]. This blockchain-based approach can enhance the transparency and traceability of security-related data, making it more difficult for malicious actors to tamper with or manipulate the information.

The integration of AI-powered analytics and anomaly detection mechanisms within the smart city management platform can further augment the security capabilities. By continuously monitoring the data flows and network activities across the Wi-Fi 6, ZigBee, and Li-Fi systems, the AI-driven algorithms can identify patterns, detect anomalies, and trigger real-time alerts to the security teams [15]. This proactive threat detection and response approach can significantly improve the smart city's ability to mitigate security incidents and protect critical infrastructure and citizen data.

The unified smart city management platform, leveraging blockchain and AI technologies, can provide the following key benefits:

1. Centralized security management: Enabling a comprehensive view of the security posture across the entire smart city ecosystem, allowing for coordinated threat response and policy enforcement [16].
2. Secure data storage and sharing: Utilizing blockchain's immutable ledger to store and share security-related data, ensuring the integrity and traceability of information [17].
3. Automated threat detection and mitigation: Employing AI-driven analytics to identify and respond to security threats in real-time, reducing the overall risk exposure.
4. Enhanced resilience and business continuity: Providing a robust and resilient platform that can withstand security incidents and maintain the availability of critical smart city services.

By integrating the security systems of Wi-Fi 6, ZigBee, and Li-Fi technologies into a unified smart city management platform, leveraging the strengths of blockchain and AI, smart city administrators can establish a comprehensive and adaptive security framework that safeguards the entire urban ecosystem.

4 Conclusion

4.1 Key Findings and Conclusions

This research study has provided a comprehensive analysis of the cybersecurity considerations surrounding the integration of Wi-Fi 6, ZigBee, and Li-Fi technologies within smart city ecosystems. The key findings and conclusions drawn from this investigation are as follows:

1. The integration of these wireless technologies in smart cities introduces a complex web of security challenges that must be addressed to ensure the confidentiality, integrity, and availability of transmitted data. Each technology possesses unique security characteristics, vulnerabilities, and mitigation strategies that require a holistic and collaborative approach to secure the overall smart city infrastructure.
2. Wi-Fi 6 offers enhanced security features, such as improved encryption, authentication, and device management, which are essential for protecting smart city networks from various threats, including unauthorized access, network congestion, and advanced persistent threats. Implementing a comprehensive security strategy that leverages these new Wi-Fi 6 capabilities is crucial.

3. ZigBee-based smart city automation systems face security risks due to their resource-constrained nature and the potential for large-scale deployments. Securing these systems requires the adoption of robust cryptographic protection, strong node authentication mechanisms, and the implementation of intrusion detection and prevention systems tailored for the unique characteristics of the ZigBee protocol.
4. Li-Fi technology, with its inherent security advantages of line-of-sight transmission and confined signal propagation, can contribute to enhancing the confidentiality of data transmission in smart city environments. However, securing Li-Fi-based communications requires the development of secure handover procedures, advanced authentication mechanisms, and comprehensive security measures to prevent threats such as eavesdropping and jamming attacks.
5. The integration of security systems across the various wireless technologies within a unified smart city management platform, leveraging emerging technologies like blockchain and artificial intelligence, can significantly improve the overall cybersecurity posture of the urban ecosystem. This approach enables centralized security management, secure data storage and sharing, and automated threat detection and mitigation.

By addressing these key findings and implementing the recommended security measures, smart city stakeholders can enhance the resilience and trustworthiness of their urban infrastructure, ensuring the protection of critical data and the well-being of citizens in the face of evolving cybersecurity threats.

4.2 Practical Implications and Industry Impact

The findings and recommendations presented in this research study have substantial practical implications for the implementation and deployment of secure smart city initiatives. The insights provided can directly inform the decisions and actions of smart city administrators, technology providers, and policymakers, ultimately contributing to the enhancement of urban security and the protection of critical data and infrastructure. From a practical standpoint, the detailed analysis of the security considerations surrounding the integration of Wi-Fi 6, ZigBee, and Li-Fi technologies can guide smart city stakeholders in the development of comprehensive security strategies and the implementation of best practices. The recommendations for robust access control, cryptographic protection, intrusion detection, and secure device management can be directly applied to strengthen the security posture of smart city wireless networks.

Furthermore, the proposed approach of integrating security systems into a unified smart city management platform, leveraging the capabilities of blockchain and artificial intelligence, provides a scalable and adaptable solution for smart city administrators. This centralized security framework can enable real-time threat monitoring, coordinated response, and the effective management of security policies across the diverse wireless technology landscape. The proposed integration of blockchain and AI into a unified smart city security management platform opens up new possibilities for creating a more resilient and adaptive cybersecurity ecosystem. By harnessing the immutability and transparency of blockchain, combined with the analytical capabilities of AI, such a platform can provide a robust and traceable security management system capable of dynamically responding to emerging threats.

The impact of this research extends beyond the immediate smart city domain, as the insights and strategies can also inform the broader technology industry. The security considerations and mitigation measures outlined in this study can contribute to the development of more secure and resilient wireless communication protocols, ultimately enhancing the overall cybersecurity landscape for various applications and industries. Integrating smart city security approaches into the wider technology ecosystem can drive innovation, promote the development of standards, and advance security best practices in wireless communications.

By adopting the recommendations and best practices presented in this research, smart city stakeholders can not only improve the security of their urban environments but also contribute to the advancement of the smart city industry as a whole. The findings can serve as a foundation for the development of new security standards, the formulation of policy guidelines, and the promotion of collaborative efforts among technology providers, research institutions, and regulatory bodies. Collaboration among diverse stakeholders is crucial for the effective implementation of the proposed security measures and ensuring they align with the dynamic needs of smart city ecosystems.

The practical implications of this research study are substantial, as they empower smart city administrators, technology developers, and policymakers to make informed decisions, implement effective security measures, and foster a more secure and resilient smart city ecosystem. The impact of these findings can be far-reaching, ultimately contributing to the creation of safer, more efficient, and more trustworthy smart cities that prioritize the protection of citizen data and critical urban infrastructure. By applying a holistic approach that encompasses technological, governance, and policy aspects, smart city stakeholders can confidently navigate the complex cybersecurity landscape and build the cities of the future that thrive on innovation while remaining resilient in the face of evolving threats.

References

1. Albreem MA, Alsharif MH, Syam S (2020) Green 5G wireless networks: a survey. Telecommun Syst 73(1):159–192
2. Ding AY, Janssen M (2020) Governance and regulations of smart cities: state-of-the-art and challenges. Inf Polity 25(2):155–172
3. Khorov E, Kiryanov A, Lyakhov A, Bianchi G (2019) A tutorial on IEEE 802.11ax high efficiency WLANs. IEEE Commun Surv Tutor 21(1):197–216

4. Salman O, Elhajj IH, Chehab A, Kayssi A (2016) ZigBee wireless sensor networks: architecture, protocols, security, and applications. In: 2016 IEEE/ACS 13th ınternational conference of computer systems and applications (AICCSA). IEEE, pp 1–6
5. Pathak PH, Feng X, Hu P, Mohapatra P (2015) Visible light communication, networking, and sensing: a survey, potential and challenges. IEEE Commun Surv Tutor 17(4):2047–2077
6. Delgado C, Canales M, Cuevas R, Gómez-Arribas FJ, Águila J (2019) A deep analysis of the Wi-Fi 6 (802.11 ax) technology and its application to 5G networks. IEEE Access 7:108765–108777
7. Blazy O, Hössler C, Kiefer F, Kreuzer S (2020) WPA3: standardizing the next generation of Wi-Fi security. In: International conference on research in security standardisation. Springer, Cham, pp 1–16
8. Wi-Fi Alliance (2019) Wi-Fi CERTIFIED enhanced open™ certification program
9. Bellalta B (2016) IEEE 802.11 ax: high-efficiency WLANS. IEEE Wirel Commun 23(1):38–46
10. Garcia-Morchon O, Kumar SS, Keoh SL, Hummen R, Struik R (2013) Security considerations in the IP-based ınternet of things. IETF Internet-Draft 19
11. Nikander P, Gehrmann C, Aura T (2003) Key authentication in ad hoc networks. In: Proceedings of the first conference on security in ad-hoc and sensor networks (SASN'03). ACM, pp 44–53
12. Hummen R, Shafagh H, Raza S, Voigt T, Wehrle K (2013) Delegation-based authentication and authorization for the IP-based ınternet of things. In: 2013 11th annual IEEE ınternational conference on sensing, communication, and networking (SECON). IEEE, pp 284–292
13. Jovicic A, Li J, Richardson T (2013) Visible light communication: opportunities, challenges and the path to market. IEEE Commun Mag 51(12):26–32
14. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: the case study of a smart home
15. Datta SK, Bonnet C, Haerri J (2017) Fog computing architecture to enable consumer centric ınternet of things services. In: 2017 ınternational symposium on consumer technologies (ISCT). IEEE, pp 65–66
16. Gupta A, Jha RK, Sharma S (2016) A survey of 5G network: architecture and emerging technologies. IEEE Access 3:1206–1232
17. Gulyamov S, Rustambekov I, Narziev O, Xudayberganov A (2021) Draft concept of the Republic of Uzbekistan in the field of development artificial intelligence for 2021–2030. Yurisprudensiya 1:107–121