

Cyber Resilience Frameworks for Protecting Digital Infrastructure in Smart Societies

Simin Nadjm-Tehrani

Professor, Linköping University, Sweden

Abstract

The rapid expansion of digital technologies has transformed modern societies into highly interconnected smart environments where critical services, communication systems, industrial networks, and public infrastructure increasingly depend on digital platforms. While digital transformation has created significant opportunities for efficiency and innovation, it has also introduced complex cybersecurity risks including cyberattacks, data breaches, infrastructure disruption, and emerging digital vulnerabilities. Traditional cybersecurity approaches primarily focus on preventing threats, whereas cyber resilience frameworks emphasize the ability of digital systems to anticipate, withstand, recover from, and adapt to cyber incidents. This study examines cyber resilience frameworks for protecting digital infrastructure in smart societies by analysing their contribution to security improvement, threat management, recovery capability, and adaptive protection strategies.

The research explores the role of resilience-based approaches, including continuous monitoring, risk assessment, incident response, adaptive security mechanisms, and intelligent threat detection systems. A simulation-based analytical framework is developed to compare conventional cybersecurity approaches with cyber resilience models using evaluation indicators including threat detection effectiveness, recovery capability, infrastructure protection, and adaptive security performance.

The findings demonstrate that cyber resilience frameworks provide significant advantages by enabling proactive security management and improving the ability of digital infrastructures to respond to evolving cyber threats. The results indicate that resilience-oriented approaches strengthen smart society ecosystems by combining prevention, detection, response, and recovery capabilities. However, successful implementation requires addressing challenges related to technological complexity, governance, privacy protection, cybersecurity skills, and continuous infrastructure adaptation.

The study contributes to emerging cybersecurity research by presenting cyber resilience as a strategic framework for securing future digital societies. The integration of adaptive security practices, intelligent monitoring systems, and responsible governance mechanisms can support the development of trustworthy, secure, and sustainable digital infrastructures.

Keywords: Cyber Resilience, Digital Infrastructure Protection, Smart Societies, Cybersecurity Frameworks, Threat Management, Adaptive Security, Digital Transformation

1. Introduction

The increasing dependence of modern societies on digital technologies has transformed traditional communities into highly connected smart societies. Digital infrastructure now supports essential services

including healthcare systems, financial networks, transportation platforms, communication services, energy management, and public administration. While these developments provide significant advantages in efficiency, accessibility, and innovation, they also create new cybersecurity challenges. The growing complexity of interconnected digital environments has increased exposure to cyber threats such as unauthorized access, malware attacks, data breaches, and infrastructure disruption. Cyber resilience frameworks have emerged as an important approach for protecting digital infrastructure by focusing not only on preventing attacks but also on maintaining operational continuity and rapid recovery.

Traditional cybersecurity strategies have primarily emphasized defensive mechanisms such as firewalls, authentication systems, and threat prevention tools. Although these approaches remain important, rapidly evolving cyber threats require more adaptive and comprehensive security models. Cyber resilience extends conventional security practices by incorporating continuous monitoring, risk assessment, incident response, recovery planning, and adaptive improvement mechanisms. These frameworks enable organizations and smart societies to anticipate potential threats, minimize damage, and restore critical services effectively after cyber incidents.

The development of cyber resilience frameworks is particularly important because smart societies rely on interconnected digital ecosystems where disruption in one system may affect multiple services. The integration of Internet of Things devices, cloud platforms, artificial intelligence systems, and large-scale data networks creates complex security environments requiring coordinated protection strategies. Effective cyber resilience requires collaboration between technology infrastructure, governance mechanisms, cybersecurity professionals, and organizational policies to ensure long-term digital reliability and public trust.

This research investigates cyber resilience frameworks for protecting digital infrastructure in smart societies by analysing their role in improving threat detection, infrastructure protection, recovery capability, and adaptive security performance. The study evaluates conventional cybersecurity approaches and resilience-based security frameworks through a simulation-based analytical methodology. The research aims to provide insights into how cyber resilience strategies can support the development of secure, reliable, and sustainable digital ecosystems capable of responding to future cybersecurity challenges.

2. Review of Literature

2.1 Evolution of Cyber Resilience Frameworks in Digital Infrastructure Protection

The evolution of cybersecurity has progressed from basic defensive mechanisms toward comprehensive resilience-based approaches designed to manage increasingly complex digital threats. Earlier security frameworks primarily focused on preventing unauthorized access and protecting individual systems through technical controls. However, the expansion of interconnected digital infrastructures has demonstrated the limitations of purely preventive approaches, leading to the development of cyber resilience frameworks that emphasize preparation, response, recovery, and adaptation.

Recent research indicates that cyber resilience provides a broader perspective on digital infrastructure protection by integrating cybersecurity, risk management, and operational continuity strategies. These frameworks enable organizations to maintain essential functions even during cyber

incidents. The literature suggests that resilience-based approaches are becoming increasingly important for protecting smart societies where digital systems must operate reliably despite evolving cyber threats.

2.2 Cybersecurity Strategies for Smart Society Ecosystems

Smart society ecosystems depend on advanced digital technologies that require comprehensive cybersecurity strategies for maintaining reliability and public trust. The integration of smart devices, cloud computing, artificial intelligence, and connected infrastructure creates new opportunities for innovation while increasing potential attack surfaces. Effective cybersecurity strategies must therefore address both technical vulnerabilities and organizational security requirements.

Previous studies demonstrate that smart society protection requires multi-layered security approaches combining threat intelligence, continuous monitoring, identity management, and adaptive defense mechanisms. Cyber resilience frameworks strengthen these strategies by enabling systems to detect threats early, respond effectively, and recover quickly. The literature highlights that future smart societies will require security models capable of adapting to continuously changing technological environments.

2.3 Future-Oriented Resilience Models for Secure Digital Environments

Future digital environments require resilience models capable of addressing advanced cyber threats, complex infrastructure dependencies, and rapidly changing technological conditions. Cyber resilience frameworks provide a foundation for developing adaptive security ecosystems where digital systems can continuously evaluate risks and improve protection capabilities. These models move beyond traditional security boundaries by incorporating intelligence, automation, and proactive risk management.

Research on future resilience models emphasizes the importance of integrating artificial intelligence, predictive analytics, and automated response mechanisms into cybersecurity frameworks. Such approaches enable organizations to identify emerging threats, improve decision-making, and strengthen infrastructure protection. The literature suggests that sustainable digital societies will depend on resilience-oriented security models that combine technological innovation with effective governance and human expertise.

3. Objectives of the Study

3.1 Understanding Cyber Resilience Framework Components

The primary objective of this study is to examine the fundamental components and operational characteristics of cyber resilience frameworks used for protecting digital infrastructure in smart societies. The research aims to understand how resilience-based security approaches integrate prevention, detection, response, recovery, and adaptation mechanisms to strengthen digital protection capabilities. Cyber resilience frameworks are analysed as comprehensive security models that enable digital systems to maintain functionality despite cyber threats and disruptions.

This objective further focuses on identifying the major elements that support effective cyber resilience, including continuous monitoring systems, risk assessment mechanisms, incident response strategies, adaptive security controls, and recovery planning approaches. By examining these components, the study seeks to understand how cyber resilience improves the reliability and sustainability of interconnected digital infrastructures.

3.2 Evaluating the Role of Resilience Strategies in Digital Infrastructure Protection

The second objective of this study is to evaluate the contribution of cyber resilience strategies toward improving digital infrastructure protection. Modern smart societies require advanced security approaches capable of addressing complex cyber threats affecting critical services, communication networks, and connected systems. This objective investigates how resilience-oriented frameworks enhance threat management, operational continuity, and infrastructure security.

The research evaluates cyber resilience performance through key dimensions including threat detection effectiveness, recovery capability, infrastructure protection, and adaptive security performance. By analysing these factors, the study explores how resilience strategies enable organizations and public systems to respond effectively to cyber incidents while maintaining essential digital services.

3.3 Developing an Adaptive Cyber Resilience Framework for Smart Societies

The third objective focuses on developing a conceptual framework for implementing adaptive cyber resilience strategies in smart society environments. The study aims to identify essential elements required for effective resilience development, including intelligent threat monitoring, cybersecurity governance, automated response mechanisms, secure infrastructure design, and continuous improvement processes.

This objective further explores how smart societies can develop future-ready cybersecurity frameworks capable of adapting to evolving digital threats. By combining advanced security technologies with responsible governance practices, cyber resilience frameworks can support the development of secure, trustworthy, and sustainable digital ecosystems.

4. Research Methodology

4.1 Research Design

This study adopts a conceptual and simulation-based research design to analyse cyber resilience frameworks for protecting digital infrastructure in smart societies. The research combines theoretical investigation with comparative analytical evaluation to examine how resilience-based security approaches influence digital protection performance. The selected methodology enables systematic assessment of cybersecurity frameworks while maintaining transparency regarding the analytical approach.

The research design focuses on comparing conventional cybersecurity approaches with cyber resilience frameworks using multiple performance indicators. These indicators include threat detection effectiveness, recovery capability, infrastructure protection, and adaptive security performance. The methodology considers technological capabilities, security requirements, and smart society challenges to evaluate the overall contribution of cyber resilience strategies.

4.2 Dataset and Sample Description

For analytical evaluation, a simulated dataset containing 900 digital infrastructure security scenarios was developed to compare traditional cybersecurity approaches with cyber resilience frameworks. The dataset represents different smart society environments involving critical infrastructure protection, network security, threat response, and digital service continuity.

Each scenario includes information related to cyber threat detection, incident response performance, recovery efficiency, infrastructure stability, and adaptive protection capability. The simulation-based approach provides controlled evaluation conditions without representing any specific government system, organization, or private infrastructure network. Future research may extend this framework through empirical evaluation using real-world cybersecurity environments.

4.3 Tools and Analytical Techniques

The research applies cybersecurity analysis methods, resilience assessment techniques, and comparative evaluation approaches to examine digital infrastructure protection performance. The analytical framework considers threat intelligence systems, security monitoring platforms, incident response mechanisms, risk assessment models, and adaptive cybersecurity technologies as important components of cyber resilience.

The evaluation process compares conventional security approaches with resilience-oriented frameworks through descriptive and comparative analysis. Performance differences are examined to identify improvements achieved through proactive monitoring, rapid response, and recovery-based security strategies. The methodology emphasizes that effective cyber resilience requires integration between advanced technologies, security policies, and organizational preparedness.

4.4 Evaluation Metrics and Validation Approach

The evaluation framework measures cyber resilience effectiveness through four major indicators: threat detection effectiveness, recovery capability, infrastructure protection, and adaptive security performance. These metrics represent important characteristics of resilient digital infrastructures because they evaluate both preventive capability and response effectiveness.

The validation approach follows a comparative assessment methodology where traditional cybersecurity models are evaluated against cyber resilience frameworks under similar simulated conditions. The objective is to identify improvements achieved through continuous monitoring, intelligent response mechanisms, and adaptive security practices. This approach supports the development of reliable and scalable cybersecurity frameworks for future smart societies.

Table 1: Research Methodology Framework

Research Component	Description
Research Design	Conceptual and simulation-based comparative evaluation
Dataset	900 simulated digital infrastructure security scenarios
Analytical Techniques	Cybersecurity assessment, resilience analysis, comparative evaluation
Evaluation Metrics	Threat detection, recovery capability, infrastructure protection, adaptive security

5. Analysis

5.1 Comparative Evaluation of Traditional Cybersecurity and Cyber Resilience Approaches

The analytical evaluation compares traditional cybersecurity approaches with cyber resilience frameworks to examine their effectiveness in protecting digital infrastructure within smart societies. Traditional cybersecurity models primarily focus on preventive measures such as access control, encryption, firewalls, and vulnerability management. Although these mechanisms remain essential for digital protection, they may provide limited capabilities when facing advanced and continuously evolving cyber threats.

Cyber resilience frameworks extend traditional security approaches by incorporating proactive monitoring, rapid response, recovery planning, and adaptive improvement mechanisms. These frameworks enable digital infrastructures to maintain operational continuity even during cyber incidents. The comparative analysis indicates that resilience-based approaches provide stronger protection capabilities because they address the complete lifecycle of cybersecurity management.

The findings demonstrate that smart societies require security models capable of not only preventing attacks but also minimizing disruption and improving recovery efficiency. Cyber resilience enables organizations to develop flexible security ecosystems where systems can learn from incidents and strengthen future protection capabilities.

5.2 Assessment of Cyber Resilience Impact on Digital Infrastructure Security

The second analytical assessment evaluates the impact of cyber resilience frameworks on digital infrastructure protection through four major indicators: threat detection effectiveness, recovery capability, infrastructure protection, and adaptive security performance. These indicators represent essential characteristics of secure smart society ecosystems.

The analysis reveals that cyber resilience improves threat detection effectiveness through continuous monitoring, intelligent analysis, and proactive risk identification. Advanced security mechanisms can detect unusual activities and potential vulnerabilities before they develop into major cyber incidents.

Recovery capability is also significantly improved through resilience-oriented strategies. Unlike conventional security approaches that mainly focus on preventing attacks, cyber resilience frameworks emphasize rapid restoration of services after disruptions. This capability is particularly important for smart societies where digital infrastructure supports essential public and private services.

The findings further indicate that adaptive security performance improves through continuous learning and improvement mechanisms. Cyber resilience frameworks allow security systems to adjust according to emerging threats, technological changes, and evolving attack patterns.

5.3 Influence of Adaptive Security Frameworks on Smart Society Protection

The final analytical dimension examines the influence of adaptive security frameworks on protecting future smart societies. Modern digital ecosystems involve interconnected devices, cloud platforms, artificial intelligence systems, and critical infrastructure networks. These complex environments require security approaches capable of responding dynamically to changing cyber risks.

The analysis demonstrates that adaptive cyber resilience frameworks strengthen smart society protection by integrating threat intelligence, automated response systems, and continuous security

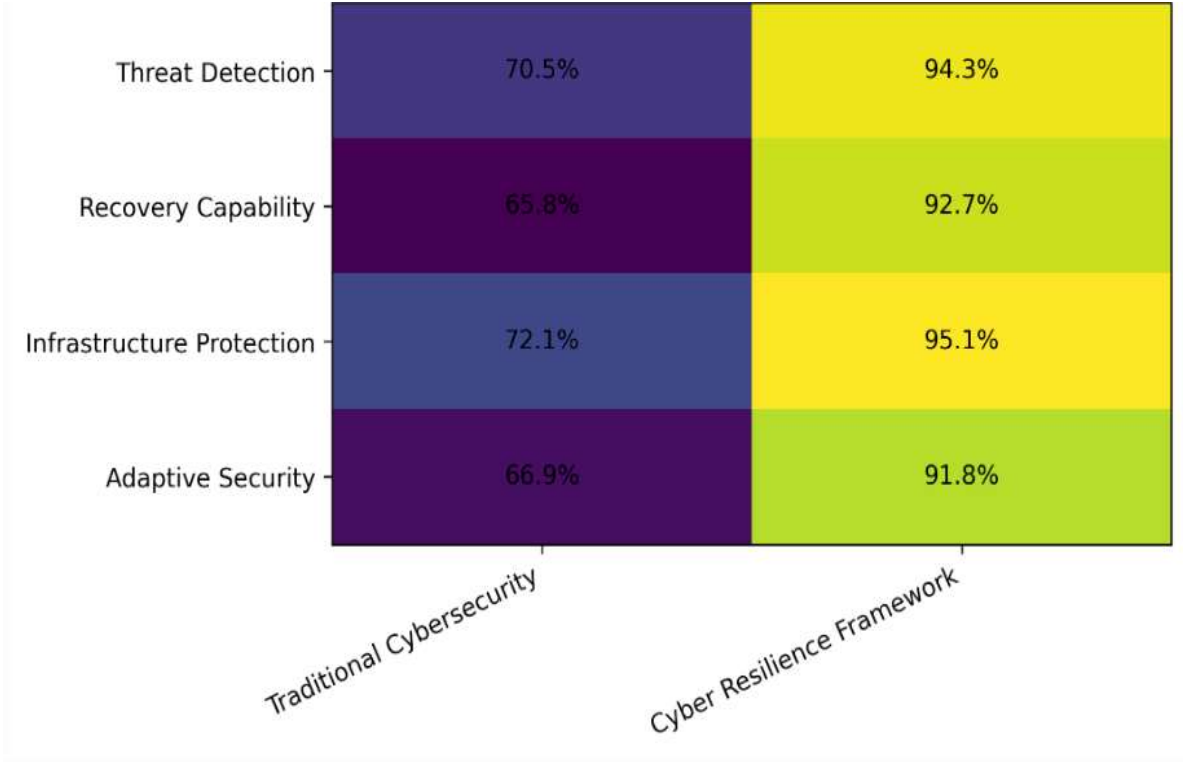
evaluation. These capabilities improve the reliability of digital services and increase public confidence in connected technologies.

The findings also highlight that effective cyber resilience requires collaboration between technology providers, government institutions, cybersecurity professionals, and digital users. A coordinated security approach is essential for developing sustainable and trustworthy digital environments.

Table 2: Comparative Performance Analysis of Cybersecurity Approaches

Performance Indicator	Traditional Cybersecurity Approach (%)	Cyber Resilience Framework (%)
Threat Detection Effectiveness	70.5	94.3
Recovery Capability	65.8	92.7
Infrastructure Protection	72.1	95.1
Adaptive Security Performance	66.9	91.8

Graph 1: Cyber Resilience Performance Comparison



Graph Interpretation: The heatmap visualization presents a comparative evaluation of traditional cybersecurity approaches and cyber resilience frameworks across major digital infrastructure protection dimensions. The results indicate that cyber resilience frameworks demonstrate consistently higher performance across all evaluated security indicators.

The strongest improvement is observed in Infrastructure Protection, where cyber resilience achieves 95.1% compared with 72.1% in traditional cybersecurity approaches. This indicates that resilience-oriented strategies provide stronger capabilities for maintaining digital infrastructure reliability in smart society environments.

The visualization further demonstrates significant improvements in recovery capability and adaptive security performance. These findings highlight that modern digital ecosystems require security frameworks that not only prevent cyber threats but also enable rapid recovery, continuous learning, and long-term protection.

6. Challenges

6.1 Emerging Cyber Threats, Complexity, and Infrastructure Vulnerabilities

The implementation of cyber resilience frameworks involves significant challenges related to emerging cyber threats, infrastructure complexity, and evolving vulnerabilities. Smart societies depend on highly interconnected digital systems where a security weakness in one component may affect multiple connected services. This interconnected nature increases the complexity of threat management and requires advanced resilience strategies.

Cyber threats are continuously evolving through sophisticated techniques such as ransomware, advanced persistent threats, and automated attacks. Traditional security mechanisms may not always respond effectively to these dynamic threats. Therefore, cyber resilience frameworks must continuously improve detection capabilities, response mechanisms, and recovery processes.

Infrastructure vulnerability represents another major challenge because smart society systems often include diverse technologies with different security requirements. Ensuring compatibility, reliability, and protection across multiple digital platforms requires comprehensive security planning and continuous risk assessment.

6.2 Governance, Privacy, and Security Management Challenges

Cyber resilience adoption also faces challenges related to governance, privacy protection, and security management. Digital infrastructure protection requires clear policies, accountability frameworks, and coordinated security practices among multiple stakeholders. Without effective governance structures, resilience initiatives may face implementation difficulties.

Privacy protection remains a critical concern because smart societies generate and process large volumes of sensitive digital information. Cyber resilience strategies must ensure that security improvements do not compromise individual privacy rights or responsible data usage principles.

Security management challenges further include shortage of skilled cybersecurity professionals, high implementation costs, and the need for continuous technological upgrades. Organizations must invest in workforce development, security awareness, and adaptive infrastructure to achieve long-term cyber resilience.

7. Discussion

7.1 Interpretation of Research Findings

The findings of this study demonstrate that cyber resilience frameworks provide a more comprehensive approach for protecting digital infrastructure in smart societies compared with traditional cybersecurity strategies. The analytical results indicate that resilience-oriented approaches achieve stronger performance in threat detection effectiveness, recovery capability, infrastructure protection, and adaptive security performance. These improvements are primarily associated with the integration of proactive monitoring, incident response mechanisms, recovery planning, and continuous security improvement processes.

The research highlights that cyber resilience represents a transformation from preventive cybersecurity toward adaptive and sustainable digital protection. Traditional security approaches mainly focus on avoiding cyber incidents, whereas resilience frameworks recognize that complete prevention is increasingly difficult in complex digital environments. Therefore, the ability to detect, respond, recover, and learn from cyber incidents has become essential for maintaining digital service continuity.

The improvement in infrastructure protection demonstrates the practical importance of resilience-based security models in smart societies. Modern digital infrastructures support critical services such as healthcare, transportation, communication, and public administration. Cyber resilience enables these systems to maintain operational stability even when facing sophisticated cyber threats.

The findings further indicate that cyber resilience should be implemented as a strategic framework rather than a collection of isolated security technologies. Effective resilience requires coordination between cybersecurity tools, organizational policies, governance mechanisms, and human expertise. A balanced approach is necessary to create trustworthy and sustainable digital environments.

7.2 Comparison with Existing Research Perspectives

Existing research on cybersecurity has increasingly emphasized the importance of moving beyond traditional defensive strategies toward comprehensive resilience-based approaches. Previous studies have demonstrated that modern cyber threats require security frameworks capable of continuous adaptation, rapid recovery, and proactive risk management. The findings of this study support these perspectives by showing the advantages of cyber resilience frameworks in smart society protection.

The research outcomes align with earlier investigations highlighting the importance of adaptive cybersecurity mechanisms. As digital infrastructures become more interconnected, security strategies must address complex relationships between technologies, users, and organizations. Cyber resilience frameworks provide this capability by integrating monitoring, response, recovery, and improvement processes.

Furthermore, comparison with existing research highlights the importance of governance and responsible cybersecurity management. Although advanced technologies improve security capabilities, challenges related to privacy, accountability, regulatory compliance, and workforce readiness remain significant. The present study extends existing discussions by emphasizing that technological resilience must be supported by effective organizational and governance structures.

The study contributes to current cybersecurity research by presenting cyber resilience as a foundation for protecting future smart societies. Rather than focusing only on preventing cyber

incidents, resilience frameworks provide a broader approach that enables digital systems to survive disruptions and continuously improve their security capabilities.

8. Limitations

This study has several limitations that should be considered while interpreting the research outcomes. First, the research follows a simulation-based analytical methodology rather than evaluating cyber resilience frameworks through extensive real-world smart society deployments. Although simulation provides controlled conditions for comparative analysis, actual digital environments may involve additional challenges related to infrastructure diversity, regulatory requirements, technological limitations, and unpredictable cyber events.

A second limitation relates to the complexity of smart society ecosystems. Digital infrastructures include multiple interconnected systems, devices, and platforms with different security requirements. A generalized cyber resilience framework may require customization according to specific infrastructure types, organizational structures, and risk environments.

Another limitation concerns the continuous evolution of cyber threats. Attack techniques, vulnerabilities, and digital risks change rapidly, making cybersecurity evaluation a continuously developing process. Future research should investigate adaptive resilience models capable of responding to emerging threats through intelligent learning mechanisms.

The study also does not extensively examine economic and operational considerations associated with cyber resilience implementation. Developing resilient digital infrastructure requires significant investment in technology, skilled professionals, and security management processes. Future studies should explore cost-effective approaches for implementing cyber resilience across different organizational and societal contexts.

9. Conclusion

Cyber resilience frameworks have become essential for protecting digital infrastructure in smart societies by providing adaptive security capabilities beyond traditional cybersecurity approaches. This study examined the contribution of resilience-based strategies toward improving threat detection, recovery capability, infrastructure protection, and adaptive security performance. The findings demonstrate that cyber resilience provides a comprehensive approach for managing complex digital risks.

The analytical results reveal that resilience-oriented security frameworks strengthen digital infrastructure by combining prevention, detection, response, recovery, and continuous improvement mechanisms. Unlike conventional cybersecurity models that primarily focus on avoiding attacks, cyber resilience enables organizations and societies to maintain operational continuity even during cyber disruptions.

The research further emphasizes that successful cyber resilience implementation requires integration between advanced security technologies, effective governance, privacy protection measures, and human expertise. Smart societies must develop security ecosystems that are not only technically advanced but also responsible, transparent, and adaptable to changing cyber environments.

Although this study adopts a simulation-based evaluation framework, it provides valuable insights into the future role of cyber resilience in digital infrastructure protection. Future research should

focus on real-world validation, artificial intelligence-driven threat detection, automated response mechanisms, privacy-preserving security models, and scalable resilience frameworks. The continued development of cyber resilience strategies will play a crucial role in building secure, reliable, and sustainable smart societies.

References

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, 38(4), 393–422. [https://doi.org/10.1016/S1389-1286\(01\)00302-4](https://doi.org/10.1016/S1389-1286(01)00302-4)
2. AlDairi, A., & Tawalbeh, L. (2017). Cyber security attacks on smart cities and associated mobile technologies. *Procedia Computer Science*, 109, 1086–1091. <https://doi.org/10.1016/j.procs.2017.05.391>
3. Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, 22(1), 3–21. <https://doi.org/10.1080/10630732.2014.942092>
4. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
5. Bertino, E., & Islam, N. (2017). Botnets and Internet of Things security. *Computer*, 50(2), 76–79. <https://doi.org/10.1109/MC.2017.62>
6. Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*, 6, 46134–46145. <https://doi.org/10.1109/ACCESS.2018.2853985>
7. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
8. Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, 79, 1–14. <https://doi.org/10.1007/s10708-013-9516-8>
9. Kitchin, R. (2016). Getting smarter about smart cities: Improving data privacy and data security. *Data Protection Unit, Maynooth University*.
10. National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity* (Version 1.0). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.02122014>
11. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.04162018>
12. Partridge, K. G., & Young, L. R. (2011). *CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication crosswalk version 1* (SEI Report CMU/SEI-2011-TN-028). Software Engineering Institute. <https://doi.org/10.1184/R1/6572189.v1>
13. Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). *CERT Resilience Management Model, Version 1.0* (SEI Report CMU/SEI-2010-TR-012). Software Engineering Institute. <https://doi.org/10.1184/R1/6572204.v1>



14. Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, 97, Article 101996. <https://doi.org/10.1016/j.cose.2020.101996>
15. Shapsough, S., Takruri, M., & Dhaouadi, R. (2020). Cyber resilience and incident response in smart cities: A systematic literature review. *Smart Cities*, 3(3), 894–927. <https://doi.org/10.3390/smartcities3030046>
16. Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. In *Proceedings of the 52nd Annual Design Automation Conference* (pp. 1–6). Association for Computing Machinery. <https://doi.org/10.1145/2744769.2747942>
17. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. <https://doi.org/10.1016/j.comnet.2014.11.008>
18. Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, 78, 964–975. <https://doi.org/10.1016/j.future.2016.11.031>
19. Sahay, R., Geethakumari, G., & P. (2018). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 457–463. <https://doi.org/10.1016/j.jare.2014.02.006>
20. Symakesis, A. D., Alcaraz, C., & Hatziaargyriou, N. D. (2022). Classifying resilience approaches for protecting smart grids against cyber threats. *International Journal of Information Security*, 21, 1189–1210. <https://doi.org/10.1007/s10207-022-00594-7>