STAP
Smart Technologies Academic Press

STAP Journal of Security Risk Management

https://www.jsrm.thestap.com/

Cybersecurity Risks and Challenges in Smart Cities: A Review with Insights for Cambodia

Mony Ho,[1] Sokroeurn Ang,[2] Sopheaktra Huy,[3] Midhunchakkaravarthy Janarthanan[4]

[1, 2, 3, 4] *School of AI Computing and Multimedia, Lincoln University College, Selangor, Malaysia*

ARTICLE INFO

Article History

Received: 30-11-2025
Revised: 30-12-2025
Accepted: 10-01-2026

Published: 13-01-2026

Vol.2026, No.1

DOI:

***Corresponding author.** **Email:** hsopheaktra.phdscholar@lincoln.edu.my

Orcid:

https://orcid.org/0009-0000-9746-5469

ABSTRACT

Smart Cities depend on interconnected digital systems, IoT devices, cloud platforms, and continuous data exchange to deliver efficient and innovative public services. However, this high level of integration increases exposure to cybersecurity risks that can disrupt essential operations and compromise citizen privacy. This review examines major cybersecurity threats affecting Smart City infrastructures, including IoT weaknesses, data exposure, DDoS attacks, surveillance system intrusion, and cloud security issues. It then analyzes Cambodia's specific challenges such as limited legal frameworks, fragmented governance, unstable infrastructure, shortages of cybersecurity skills, and financial constraints. Global frameworks including the NIST Cybersecurity Framework, Zero Trust Architecture, IoT security models, and Smart City security architectures are reviewed to identify best practices. A gap analysis highlights significant differences between international standards and Cambodia's current readiness. Finally, the study proposes strategic recommendations to strengthen national policies, enhance technical and human capability, and improve infrastructure resilience. The findings provide valuable guidance for policymakers and stakeholders seeking to advance secure and sustainable Smart City development in Cambodia.

Keywords: Cybersecurity, Smart Cities, Critical Infrastructure Protection, IoT Security, Cloud Security

How to cite the article

1. Introduction

1.1 Smart City Definition

A Smart City is an urban ecosystem that integrates information and communication technologies (ICT), Internet of Things (IoT) devices, cloud platforms, and data analytics to improve operational efficiency, public service delivery, and citizen well-being [1]. Through continuous data collection and interconnected digital infrastructure, Smart Cities support functions such as transportation management, environmental monitoring, public safety enhancement, and digital governance [2]. The effectiveness of a Smart City depends not only on the sophistication of its technology but also on its ability to manage, secure, and govern these systems responsibly [3].

1.2 Importance of Cybersecurity in Smart Cities

Cybersecurity is fundamental to Smart City success because digital interconnectivity significantly expands the attack surface. Vulnerabilities in IoT devices, surveillance systems, cloud services, and communication networks create opportunities for cyberattacks that can disrupt critical services, expose sensitive data, and compromise public trust [4]. Threats such as DDoS attacks, unauthorized access to CCTV systems, malware infiltration, and large-scale data breaches pose serious risks to city operations [5]. As Smart Cities rely on uninterrupted digital communication and real-time data exchange, ensuring the confidentiality, integrity, and availability of these systems becomes essential for safety and resilience [6].

1.3 Cambodia's Smart City Transformation

Cambodia is actively advancing Smart City initiatives through national programs such as the Phnom Penh Master Plan 2035 and the Siem Reap Smart City development project. These initiatives aim to modernize transportation systems, strengthen public safety, improve waste management, and enhance digital governance using ICT and IoT technologies. However, Cambodia faces notable cybersecurity challenges, including unstable Internet connectivity, inconsistent electricity supply, limited cybersecurity expertise, and the absence of a comprehensive data protection law. As digital services rapidly expand, the cybersecurity capacity of Cambodia must evolve to support secure and sustainable Smart City growth [7],[8].

1.4 Motivation for the Study

The motivation for this review stems from the increasing cybersecurity risks associated with Smart City environments, particularly in developing nations that are transitioning toward digital governance. Earlier analysis highlighted several vulnerabilities such as IoT weaknesses, data privacy risks, and real incidents like the large-scale DDoS attack on Cambodia's leading ISPs, all of which demonstrate the urgency of strengthening Smart City security. In addition, ethical concerns, legal limitations [9], and gaps in national governance further emphasize the need for a structured review that examines cybersecurity threats and identifies solutions that are suitable for Cambodia's Smart City context.

1.5 Objectives of the Study

This review aims to achieve the following objectives:
1. To examine major cybersecurity risks associated with Smart City infrastructures.
2. To analyze Cambodia's unique cybersecurity challenges during Smart City development.
3. To review global cybersecurity frameworks relevant to securing Smart Cities.
4. To highlight gaps in Cambodia's legal, technical, and governance structures.
5. To provide strategic recommendations for strengthening Smart City cybersecurity within the Cambodian context.

2. Cybersecurity Risks

2.1 IoT Vulnerabilities

Smart Cities rely heavily on IoT devices and sensors to support real time data collection for transportation systems, public safety, environmental monitoring, and municipal operations. However, these devices often lack strong built in security

controls, making them highly vulnerable to attacks. Weak authentication, insecure firmware, and unprotected communication channels expose Smart City IoT networks to unauthorized access and device manipulation. The complexity and scale of IoT deployments further increase the difficulty of monitoring and securing thousands of interconnected devices, raising the likelihood of data exposure and operational disruption [10], [11].

2.2 Data Exposure and Privacy Risks

Smart City platforms generate and process vast volumes of data, including environmental information, public mobility patterns, and in some cases sensitive citizen data. Without strong data governance and security mechanisms, these large datasets become attractive targets for cybercriminals. Insufficient encryption, data storage vulnerabilities, and unregulated data sharing practices can result in significant privacy breaches. Such incidents undermine citizen trust and may lead to harmful consequences when personal information or city infrastructure data is exposed to unauthorized entities [12], [13].

2.3 Distributed Denial of Service (DDoS) Attacks

Smart City operations depend on continuous connectivity and system availability. This makes them particularly vulnerable to Distributed Denial of Service (DDoS) attacks, which overload critical infrastructure and disrupt essential digital services. Cambodia has previously experienced a large-scale DDoS incident that reached approximately 150 Gbps and affected major national Internet service providers. Such attacks demonstrate how a well-coordinated DDoS assault could overwhelm Smart City platforms, interrupt transportation systems, disable public service dashboards, or block communication between IoT devices and central monitoring systems [14].

2.4 CCTV and Surveillance System Attacks

CCTV systems play a central role in Smart City security by supporting traffic monitoring, crime prevention, and public safety. However, insecure camera configurations, default credentials, and unprotected transmission channels make surveillance systems vulnerable to hacking. Unauthorized access to CCTV feeds may allow attackers to manipulate or intercept video streams, disable monitoring zones, or invade citizen privacy. These risks directly affect public safety and undermine the reliability of digital surveillance as a Smart City tool [15],[16].

2.5 Cloud and Data Storage Security Issues

Smart Cities increasingly depend on cloud platforms to store and process large datasets collected from IoT devices and municipal systems. While cloud services provide scalability, they also introduce risks related to misconfigured storage environments, weak access controls, and vulnerable APIs. When encryption is not consistently applied, sensitive data may be exposed to unauthorized users or external attackers. Mismanagement of cloud policies can also result in data leaks, loss of service availability, and widespread operational disruption across multiple Smart City subsystems [17], [18].

3. Challenges in Cambodia

3.1 Legal and Regulatory Challenges

Cambodia's Smart City development is constrained by the absence of a comprehensive data protection law and the limited enforcement of existing digital regulations. While the E-commerce Law partially addresses electronic data handling, it does not provide clear guidelines for safeguarding personal data collected through Smart City systems. The country is also in the process of drafting a cybersecurity law, but it has not yet been implemented at a national level. This regulatory gap creates uncertainty in data governance and hampers the establishment of standardized cybersecurity practices, resulting in vulnerabilities across IoT networks, surveillance systems, and cloud-based Smart City platforms [19].

3.2 Governance and Institutional Challenges

Effective Smart City cybersecurity relies on coordinated governance structures, including centralized monitoring, incident response capabilities, and clear accountability mechanisms. Cambodia currently faces fragmentation in digital policy implementation, with responsibilities distributed across multiple ministries and agencies. This dispersion limits the country's ability to detect, respond to, and recover from cyber incidents in a unified manner. The absence of a national Security Operations Center (SOC) or coordinated critical infrastructure monitoring system further weakens resilience to cyberattacks targeting public services [20].

3.3 Human Resource and Capacity Challenges

A significant barrier to Smart City cybersecurity readiness is the limited availability of trained cybersecurity professionals. Cambodia faces shortages in expertise related to IoT security, cloud security, network defense, and digital forensics. Smart City technologies require advanced technical competencies to manage risks associated with large-scale data systems and interconnected infrastructures. Without substantial investment in cybersecurity education and workforce development, the implementation and maintenance of secure Smart City systems remain difficult [21], [22].

3.4 Infrastructure and Connectivity Limitations

Smart Cities depend on stable and high-capacity Internet networks as well as reliable electricity supply. Cambodia's infrastructure still experiences connectivity fluctuations, bandwidth limitations, and occasional power outages, all of which pose risks to digital services and IoT systems. Unstable networks affect real-time communication between devices and central platforms, while power interruptions may disrupt critical Smart City operations such as traffic monitoring, safety systems, or emergency response platforms. The lack of redundant backup systems further reduces the country's ability to maintain service availability during disruptions [23].

3.5 Financial and Resource Constraints

Developing a secure Smart City requires sustained investment in cybersecurity technologies, skilled personnel, and resilient infrastructure. However, the high cost of advanced security tools, IoT protections, and cloud service hardening presents financial challenges for Cambodia as a developing nation. Limited national budgets and dependence on external support restrict the scale and speed of cybersecurity adoption. Without sufficient funding, the deployment of encryption systems, intrusion detection tools, backup infrastructure, and secure data governance frameworks remains slow and uneven [24].

4. Existing Frameworks

4.1 NIST Cybersecurity Framework

The NIST Cybersecurity Framework (NIST CSF) is one of the most widely adopted security standards for critical infrastructure protection. It is built around five core functions that provide a comprehensive approach to managing cybersecurity risks [25], [26].

4.1.1 Identify

This function emphasizes understanding assets, systems, people, data, and risks. For Smart Cities, the identification of IoT devices, communication networks, and data flows is essential for detecting vulnerabilities and establishing baseline security requirements.

4.1.2 Protect

The protection function includes access control, cybersecurity training, data security, encryption, and maintenance. Smart City environments benefit from protective technologies such as network segmentation, secure device authentication, and encryption of sensitive citizen data.

4.1.3 Detect

Detection involves establishing monitoring systems to identify cybersecurity events in real time. Smart Cities require continuous monitoring of IoT devices, cloud resources, and public infrastructure systems to detect anomalous behavior early.

4.1.4 Respond

This function focuses on appropriate action during a cyber incident. For Smart Cities, coordinated response is crucial because multiple interconnected services may be impacted simultaneously.

4.1.5 Recover

The recovery function ensures timely restoration of critical services after an incident. Smart Cities require robust disaster recovery plans, data backups, and system redundancies to restore operations and maintain public trust.

4.2 Zero Trust Architecture (ZTA)

Zero Trust Architecture is a modern cybersecurity model based on the principle of never trusting and always verifying. It assumes that threats may come from both outside and inside the network [27], [28].

4.2.1 Identity Verification

Zero Trust enforces strict identity verification for every device, user, and system component. In Smart Cities, this prevents unauthorized access to IoT sensors, surveillance cameras, and cloud platforms.

4.2.2 Micro Segmentation

This approach divides networks into isolated segments to reduce the spread of attacks. In Smart City environments with thousands of interconnected systems, micro segmentation limits the impact of compromised devices.

4.2.3 Least Privilege Access

Zero Trust restricts access rights to only what is necessary. Applying least privilege reduces the risk of privilege misuse or lateral movement within Smart City systems.

4.3 IoT Security Frameworks

IoT security frameworks provide guidelines for protecting devices that often have limited built in security.

4.3.1 Secure Boot and Firmware Validation

Secure boot ensures that devices only run trusted firmware. This prevents malicious code injection into Smart City IoT devices.

4.3.2 Device Identity Management

Unique digital identities allow centralized authentication and monitoring of IoT devices, enabling rapid detection of unauthorized or cloned devices.

4.3.3 End to End Encryption

Encrypting data from the device to the cloud protects sensitive information from interception and modification during transmission [29]-[31].

4.4 Smart City Security Models

4.4.1 Cyber Physical Systems (CPS) Security Architectures

CPS security models safeguard systems that integrate digital processes with physical infrastructure. Examples include traffic lights, public transport systems, and power distribution networks. These models focus on resilience, anomaly detection, and safe recovery.

4.4.2 Multi-Layer Smart City Security Models

Several studies propose multi-layer architectures that secure Smart Cities across device, network, application, and governance layers. These models align well with the layered nature of Smart City technologies.

4.4.3 Resilience and Continuity Approaches

Resilience focused models emphasize maintaining essential services even during cyberattacks. Backup systems, redundant communication channels, and automated failover mechanisms support continuity in Smart *City operations [32], [33].*

4.5 Data Governance and Privacy Models

4.5.1 GDPR Principles

European GDPR principles influence global privacy regulation and stress accountability, transparency, and data minimization. These principles are relevant for Smart Cities that process large amounts of citizen data.

4.5.2 Privacy by Design

This model integrates privacy considerations into system design from the outset. Smart City applications can adopt this approach to reduce privacy risks associated with surveillance and data collection.

4.5.3 Data Minimization and Transparency

Limiting unnecessary data collection and informing citizens about how their data is used enhance trust and reduce privacy exposure. These principles guide ethical and secure Smart City data practices [34], [35].

5. Gap Analysis: Implications for Cambodia

5.1 Gap Between Global Standards and Cambodia's Smart City Readiness

Global cybersecurity standards such as the NIST Cybersecurity Framework, ISO 27001, Zero Trust Architecture, and IoT security guidelines provide comprehensive models for managing cybersecurity risks. However, Cambodia's current Smart City development does not yet fully align with these standards. While national initiatives aim to modernize urban infrastructure, the absence of mandatory security requirements for IoT deployment, cloud usage, surveillance systems, and data management creates a significant gap between global best practices and local implementation.

5.2 Legal and Regulatory Gaps

Cambodia lacks a dedicated data protection law, and existing digital regulations do not sufficiently address Smart City cybersecurity requirements. The E-commerce Law offers general guidance on electronic data but does not provide clear rules for data privacy, IoT security, cloud protection, or incident response. The ongoing development of a national cybersecurity law indicates progress, but the delay in implementation leaves Smart City systems without a robust legal foundation. As a result, government agencies and private developers lack clear obligations regarding secure system design and citizen data protection.

5.3 Technical and Infrastructure Gaps

Many Smart City services rely on stable Internet connectivity, reliable electricity, and secure networks. Cambodia's digital infrastructure still suffers from intermittent Internet quality, limited bandwidth, and periodic power outages. These limitations weaken system availability and resilience, especially during emergencies or cyberattacks. Moreover, Smart City deployments often depend on third-party cloud services, but Cambodia has not yet established national guidelines for cloud security configuration, encryption standards, or secure data hosting requirements.

5.4 Cybersecurity Workforce and Skills Gaps

Advanced Smart City systems require skilled professionals capable of managing IoT security, cloud security, threat detection, and incident response. Cambodia faces a shortage of cybersecurity experts, and existing training programs do not yet meet the demands of large scale digital infrastructure projects. Without sufficient human resource capacity, vulnerabilities in Smart City systems may go undetected, and response to cyber incidents may be slow or ineffective.

5.5 Governance and Coordination Gaps

Smart City cybersecurity requires coordinated oversight across ministries, municipal authorities, telecommunications providers, and technology developers. However, Cambodia's governance structure for cybersecurity remains fragmented, with responsibilities distributed across multiple agencies. The absence of a centralized national Security Operations Center (SOC), unified monitoring framework, or standardized reporting mechanisms makes it difficult to achieve timely detection and coordinated response to cyber threats. This governance gap significantly increases risk for interconnected Smart City services.

5.6 Risk of Rapid Digital Growth Without Strong Security Foundations

Cambodia is progressing quickly in Smart City development, yet cybersecurity maturity is advancing more slowly. Rapid adoption of IoT devices, cloud platforms, and surveillance technologies without adequate security controls increases the likelihood of system compromise. This imbalance between innovation and security can lead to operational disruption, misuse of citizen data, and long-term trust issues. The real-world DDoS attack on major Cambodian ISPs highlights the consequences of insufficient cyber preparedness and emphasizes the need for a stronger cybersecurity foundation.

5.7 Strategic Need for National Cyber Policies

The gap analysis reveals an urgent need for Cambodia to develop comprehensive national cybersecurity policies that address Smart City requirements. This includes formalizing data protection legislation, defining IoT security standards, establishing requirements for cloud and network security, and implementing national level monitoring systems. Such policies are essential not only for protecting Smart City infrastructures but also for enabling safe digital transformation across the country.

6. Recommendations

6.1 Establish Comprehensive National Cybersecurity Legislation

Cambodia should accelerate the development and adoption of national cybersecurity laws that clearly define cybersecurity obligations for government agencies, private operators, and Smart City developers. A dedicated legal framework must include requirements for secure IoT deployment, incident reporting, data protection, and cloud security. Establishing cybersecurity standards at the national level will help ensure consistent implementation across all Smart City projects.

6.2 Develop a National Data Protection Law

A robust data protection law is essential for safeguarding personal and sensitive information collected through Smart City systems. Such legislation should define the rights of citizens, obligations of data controllers, limitations on data usage, and penalties for misuse or breaches. Incorporating principles like consent, purpose limitation, and transparency would strengthen public trust and ensure responsible data handling across Smart City applications.

6.3 Implement IoT Security Standards and Certification

Given the critical role of IoT devices in Smart Cities, Cambodia should adopt IoT security standards that mandate secure boot, encryption, device authentication, and regular firmware updates. Introducing certification requirements for IoT vendors can ensure that devices used in Smart City infrastructure meet minimum cybersecurity criteria. This measure will reduce the risk of IoT-based attacks and strengthen the overall integrity of the ecosystem.

6.4 Expand Cybersecurity Workforce Development

Building a skilled cybersecurity workforce is essential for long-term Smart City resilience. Universities and technical institutes should integrate cybersecurity, IoT security, and cloud security into their curricula. Government programs and industry partnerships can support professional training, certifications, and capacity-building initiatives. Increasing the number of skilled cybersecurity professionals will enhance Cambodia's ability to manage and secure Smart City systems.

6.5 Establish a National Security Operations Center (SOC)

A centralized SOC would significantly improve Cambodia's ability to monitor cyber threats, coordinate incident response, and protect national digital infrastructure. The SOC should incorporate real-time monitoring, threat intelligence sharing, and coordinated response mechanisms across sectors. Such a center would enhance cyber situational awareness and support early detection of attacks on Smart City services, critical infrastructure, and government systems.

6.6 Strengthen Cloud and Network Security Policies

Smart City systems heavily rely on cloud services and digital communication networks. Cambodia should introduce national cloud security guidelines that include encryption requirements, secure configuration standards, multi-factor authentication, and continuous monitoring. Similarly, network security policies must incorporate segmentation, intrusion detection systems, and redundancy measures to minimize disruption during cyber incidents.

6.7 Improve Infrastructure Resilience through Backup Systems

Smart City operations require stable and reliable connectivity. To enhance availability, Cambodia should invest in redundant Internet connections, backup power systems, and failover mechanisms for critical Smart City services. This includes deploying uninterruptible power supplies, generators, and multi-ISP connections to ensure service continuity during outages. Strengthening infrastructure resilience will help reduce the impact of attacks such as DDoS incidents or power failures.

6.8 Promote Public Awareness and Digital Ethics

Public understanding of cybersecurity and digital ethics is essential for the success of Smart City initiatives. Awareness campaigns, community workshops, and educational programs can help citizens understand privacy risks, safe digital behaviors, and the role of cybersecurity in Smart City environments. Promoting transparency and responsible data use will foster trust and support citizen participation in Smart City programs.

6.9 Strengthen Regional and International Collaboration

Cambodia can benefit from collaborating with ASEAN, international cybersecurity agencies, and global technology partners. These collaborations can provide access to advanced cybersecurity knowledge, best practices, training programs, and threat intelligence. Strengthening regional and global cooperation will help Cambodia adapt to emerging cyber threats and accelerate the adoption of secure Smart City technologies.

7. Conclusion

Smart Cities offer valuable opportunities to enhance public services, improve operational efficiency, and support sustainable urban development. At the same time, the integration of IoT devices, cloud systems, surveillance technologies, and interconnected platforms increases cybersecurity risks. This review identified key vulnerabilities, including IoT weaknesses, large scale data exposure, DDoS attacks, surveillance system intrusion, and cloud security challenges. Cambodia's progress toward Smart City development is affected by limited regulations, fragmented governance, shortages in cybersecurity expertise, unstable digital infrastructure, and financial constraints. Comparing these conditions with global frameworks such as the NIST Cybersecurity Framework, Zero Trust Architecture, IoT security models, and Smart City security architectures reveals substantial gaps in national readiness. Addressing these weaknesses requires coordinated national action, including stronger laws, a data protection framework, improved IoT and cloud security standards, investments in digital resilience, and development of cybersecurity skills. Establishing a national security operations center and expanding regional collaboration will further strengthen national capacity. By prioritizing these measures, Cambodia can build a secure and trustworthy Smart City environment that protects critical systems and supports long term digital transformation.

Corresponding author
Sopheaktra Huy
hsopheaktra.phdscholar@lincoln.edu.my

Acknowledgements
NA.

Funding
No funding.

Contributions
SH; SA; MH; VB; Conceptualization, SH; SA; MH; VB; Investigation, SH; SA; MH; VB; Writing (Original Draft), SH; SA; MH; VB; Writing (Review and Editing) Supervision, SH; SA; MH; VB; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

References

[1] Kociuba, D., Sagan, M., & Kociuba, W. (2023). Toward the smart city ecosystem model. *Energies, 16*(2795), 1–26.
[2] Oladimeji, D., Gupta, K., Kose, N. A., Gundogan, K., Ge, L., & Liang, F. (2023). Smart transportation: An overview of technologies and applications. *Sensors, 23*(3880), 1–32.
[3] Gharaibeh, A., et al. (2017). Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys & Tutorials, 19*(4), 2456–2501.
[4] Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security, 4*, 65–88.
[5] Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. *Applied Sciences, 13*(790), 1–36.
[6] Tcholtchev, N., & Schieferdecker, I. (2021). Sustainable and reliable information and communication technology for resilient smart cities. *Smart Cities, 4*(1), 156–176.
[7] Royal Government of Cambodia. (2021). *General guidelines for provincial administration (2020–2030)*. Phnom Penh, Cambodia.
[8] Sar, V. (2023). *Digital government in Cambodia: Challenges and solutions*. KDI School of Public Policy and Management.
[9] Chang, V. (2020). *An ethical framework for big data and smart cities*. School of Computing, Engineering and Digital Technologies, Teesside University.
[10] Musa, A. A., Malami, S. I., Alanazi, F., Ounaies, W., Alshammari, M., & Haruna, S. I. (2023). Sustainable traffic management for smart cities using Internet-of-Things-oriented intelligent transportation systems (ITS): Challenges and recommendations. *Sustainability, 15*(9859), 1–15.
[11] Alotaibi, A., Aldawghan, H., & Aljughaiman, A. (2025). A review of the authentication techniques for Internet of Things devices in smart cities: Opportunities, challenges, and future directions. *Sensors, 25*(1649), 1–43.
[12] Gasana, A. D., et al. (2023). A review of smart city data governance, privacy protection, and cybersecurity challenges. *Future Internet, 15*, 1–23.
[13] Ahn, J., Hussain, R., Kang, K., & Son, J. (2025). Exploring encryption algorithms and network protocols: A comprehensive survey of threats and vulnerabilities. *IEEE Communications Surveys & Tutorials*.
[14] Khiev, S. (2023). *Cybersecurity landscape and digital resilience in Cambodia*. SSRN.
[15] Vennam, P., T. C., P. T., B. M., T. B. M., Kim, Y.-G., & N., P. K. B. (2021). Attacks and preventive measures on video surveillance systems: A review. *Applied Sciences, 11*(5571), 1–17.
[16] Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. (2020). The security of IP-based video surveillance systems. *Sensors, 20*(4806), 1–25.
[17] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*, 1–11.
[18] Dawood, M., et al. (2023). Cyberattacks and security of cloud computing: A complete guideline. *Symmetry, 15*(1981).
[19] Savuth, C., & Sothea, O. (2023). Digital transformation in Cambodia: Policies, strategies, supporting factors and infrastructure. *Journal of Southeast Asian Economies, 40*(1), 145–172.
[20] Mono, O. C. (2021). E-government in Cambodia: Challenges and practical paths to achieve a functional e-government. *Cambodia Development Center, 3*(2), 1–19.
[21] Asian Development Bank. (2025). *Asia digital transformation: Country perspectives – Cambodia*.
[22] Ramim, M. M., & Hueca, A. (2021). Cybersecurity capacity building of human capital: Nations supporting nations. *Online Journal of Applied Knowledge Management, 9*(2), 65–85.
[23] World Bank Group, & GFDRR. (2024). *Cambodia: Geospatial analysis for resilient road accessibility for human development and logistic supply*. Washington, DC.
[24] Hill, H., & Menon, J. (2013). *Cambodia: Rapid growth with institutional constraints* (SSRN Working Paper No. 331). Asian Development Bank.

[25] Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb model. *Journal of Cybersecurity*, *6*(1), 1–8.
[26] Bernardo, L., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. *Electronics*, *14*(1364), 1–20.
[27] Chinnasamy, S. R., & Janakiraman, S. N. (2022). *Zero trust architecture: A systematic literature review*.
[28] Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. *IEEE Access*, *11*, 19487–19512.
[29] Karie, N. M., et al. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, *9*, 121975–121999.
[30] Alghareeb, M. S., Almaiah, M., & Badr, Y. (2024). Cyber Security Threats in Wireless LAN: A Literature Review. International Journal of Cybersecurity Engineering and Innovation, 2024(1).
[31] Lohr, S. K., et al. (2020). IoT security framework overview. *Computers*, *9*(44), 1–20.
[32] Alrajeh, M., Almaiah, M., & Mamodiya, U. (2026). Cyber Risk Analysis and Security Practices in Industrial Manufacturing: Empirical Evidence and Literature Insights. International Journal of Cybersecurity Engineering and Innovation, 2026(1).
[33] Ali, A., et al. (2022). Advanced security framework for Internet of Things (IoT). *Technologies*, *10*(60), 1–17.
[34] Al-shareeda, M., & Alrudainy, H. (2026). Sustainable and Secure Energy Optimization Strategies in the Internet of Healthcare Things (IoHT). International Journal of Cybersecurity Engineering and Innovation, 2026(1).
[35] Atlam, A. A. A., & Alenezi, A. G. (2021). Security and privacy in smart cities: Challenges and opportunities. *Journal of Network and Computer Applications*, *182*, 1–20.
[36] Chatterjee, R. K., Sharma, P. K., & Park, J. H. (2021). Cybersecurity for smart cities: Challenges and solutions. *Multimedia Tools and Applications*, *80*, 17343–17372.
[37] Chandak, A., & Chandak, P. (2026). Blockchain technology in health care an extensive scoping review of the existing applications, challenges, and future directions. International Journal of Cybersecurity Engineering and Innovation, 2026(1).
[38] Liu, F. (2022). Social data governance: Towards a definition and model. *Journal of Information Science*.
[39] Kuzio, J., et al. (2022). Building better global data governance. *Data & Policy*, *4*, e25.

Biographies

Mony Ho. Mony Ho is a Ph.D. candidate in Information Technology at Lincoln University College, Malaysia. He holds a Master's degree in IT and Data Science from the European International University, France. He is currently a senior technical teacher at Preah Kossomak Polytechnic Institute and lectures part-time at multiple universities in Cambodia. His teaching and research interests include Data Science, Big Data, software engineering, cloud technologies, and web and mobile application development. https://orcid.org/0009-0004-3389-1951

Sokroeurn Ang. Mr. Sokroeurn Ang is a senior lecturer in cybersecurity. He has been teaching ICT and cybersecurity since 2015 and has held various roles in ICT and cybersecurity for over a decade. His professional experience spans the central banking sector, private banking, and internet service providers. He has been actively involved in areas such as cybersecurity risk assessment, IT governance, network security, web application security, cybersecurity incident response, BCP and DRP, cloud security, VAPT, and IT auditing. Mr. Sokroeurn Ang completed a Micro-Master in Cybersecurity at the Rochester Institute of Technology (RIT), USA, and earned a Master's degree in Cybersecurity from Royal Holloway, University of London, UK. He is currently pursuing a PhD in Cybersecurity at the Lincoln University College, Malaysia. Mr. Sokroeurn Ang has been certified such as CISSP, CISA, CISM, CC, ECSA, CEH, CCNA Security, CCNA, CyberOps, and AWS Certified Cloud Practitioner. In addition, he is a certified Cisco Instructor and an AWS Academy Instructor. https://orcid.org/0009-0000-9746-5469

Mr. Sopheaktra Huy is a Ph.D. candidate in Cyber Security at Lincoln University College, Malaysia. He holds an M.Sc. in IT from the Royal University of Phnom Penh and an MBA from Asia Euro University, Cambodia. He is currently the IT Risk Manager at Wing Bank and has previously held senior roles at WB Finance, Phillip Bank, and PRASAC MFI. With over 20 years of part-time lecturing experience, he has taught programming, cyber risk, and IT project management. He holds certifications in CISA, CISM, and CEH, with research interests in IT automation and cybersecurity governance.
Email: hsopheaktra.phdscholar@lincoln.edu.my

Dr. Vivekanandam Balasubramaniam is the Deputy Dean of the School of AI Computing and Multimedia at Lincoln University College, Malaysia. He has authored over 47 publications with 420+ citations, focusing on artificial intelligence, machine learning, cybersecurity, and cloud computing. His work includes both research papers and patents, contributing significantly to innovation and academic development in these fields. Dr. Vivekanandam Balasubramaniam also serves as a research supervisor and mentor for numerous postgraduate students, supporting innovative work in artificial intelligence and cloud-based systems. https://orcid.org/0000-0002-5534-2142