International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AI THREAT MODELLING IN LOCAL GOVERNMENT: ADVANCING CYBERSECURITY THROUGH REGULATORY FRAMEWORKS AND GOVERNANCE

Santosh Pai[1*], Srinivasa Rao Kunte R[2]

[1]Research Scholar, Department of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India

*Corresponding Email Id: g.santoshpai@gmail.com

Orcid Id: 0000-0002-5053-1673

[2]Research Professor, Department of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India

Email Id: drsrinivasaraokunte@srinivasuniversity.edu.in

Orcid Id: 0000-0002-5062-1505

Abstract

Local governments are no longer facing smart but unsophisticated threats but have become confronted by highly intelligent and automated threats because of fast-paced digitalization, aged IT infrastructure, and scarce cybersecurity talent. Smaller municipalities experience a larger number of incidents of AI (Artificial Intelligence) powered cyberattacks than larger governmental organizations but are incapable of leveraging the regulatory harmonization and technical capabilities for countering such threats. This paper advances a conceptual AI-enabled threat modelling architecture uniquely developed for the local government context by incorporating generative AI functionalities with current cybersecurity basic standards such as GDPR, NIST, and ISO 27001. Differing from typical threat modelling frameworks that have high false positives and are incapable of reflecting regulatory accountability, the introduced governance-compliant model utilizes AI for the automated detection of threats, generation of mitigation stories, and assistance for legal transparency needs. The research amalgamates global policy evolutionary work, cybersecurity governance texts, and ethical guidelines for AI to develop a regulatory-compliant architecture that increases explainability, accountability, and traceability of the cybersecurity operations for municipalities. By integrating AI threat detection efficiency with legal structures for compliance, the research advocates for a futuristic paradigm that enables local governments to realize cyber resilience achieving greater regulatory oversight and ethical certainty. The theoretical synthesis proposed in this paper uses generative AI in threat modeling in the areas of autonomous threat description, generation of mitigations, and compliance ready reporting. The proposed threat modeling approach is generalized and governance focused. It also conceptually demonstrates reduced false positives and improved accountability.

Keywords: *Artificial Intelligence; Compliance; Regulatory Frameworks; Threat Modelling; AI Governance and Cybersecurity*

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

INTRODUCTION

As the digital landscape grows, small local governments become more vulnerable to many more cyber security threats. Although larger organizations may garner media attention for hacks, or make national news, smaller municipalities face a unique set of challenges stemming from their structure that makes them susceptible to hacks. Limited budgets, outdated hardware, and a lack of qualified IT personnel have all contributed to municipalities being positive targets. The implications of a successful hack are significant, as sensitive data could be compromised as much critical services that communities rely on daily. It is important to call attention to the underlying issues that feed this threat as you work to support both safety and resilience in your community in an increasingly connected world (Norris and Mateczun, 2022).

Municipal leaders are witnessing a concerning rise in cyberattacks, as municipalities are used as target for both ransomware and data theft. Cyberattacks often lead to loss of sensitive information, as well as disrupting municipal operations leading to vulnerabilities to the community (Wolff and Lehr, 2018). Because these small communities are not ready for the threat that cyberattacks pose, however, they typically fall victim to misuse of personally identifiable information and financial records of its citizens. As cyber threats evolve and change, the preparation gap grows between larger organizations and small communities, justifying a plea for more help and speed. The damage of a cyberattack for a small local municipality can be even more serious and can be difficult to assess if the municipality found itself in a cyber crisis (Hatcher et al. 2020). Disruption from successful incursion can lead to broken chains of trust and compromise of citizen data including personal details and financial records and possibly identity theft and infringing on rights of privacy (Chaudhuri et al., 2023). Improvements in cybersecurity decisions is where artificial intelligence systems are becoming more and more prevalent.

The technologies are able to address a broad spectrum of threats effectively and automate accurate incident response strategies (Yigitcanlar et al., 2023). This evolution is crucial for addressing the swiftly changing landscape of cyber threats, with the difficulty of managing huge amounts of threat intelligence data. AI-driven threat detection is exceptionally efficient; but, hackers continuously adapt their attack methodologies to circumvent it. They use each other to initiate more potent cyberattacks employing sophisticated methods such as polymorphic malware, zero-day exploits, and phishing campaigns utilising generative AI. AI-driven threat detection aims to counteract changing threat strategies that are challenging to identify and address, including the proliferation of attack vectors such as IoT devices, cloud infrastructures, and mobile platforms. The aim is to address the increased rate and rapid rate of cyberattacks, especially ransomware (Yigitcanlar et al., 2023).

It will be useful to look at the comparative sector data depicted in Figure 1 to show that while the local governments are given lower attention in the cybersecurity discussion, they are having roughly twice the higher incidents than the federal agencies, owing it to their inability to achieve regulatory conformity and inadequate investment of resources. The challenge

Received: August 14, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

encompassed not only cybersecurity in AI governance but also larger concerns like ethical AI deployment, transparency, and adherence to privacy legislation.

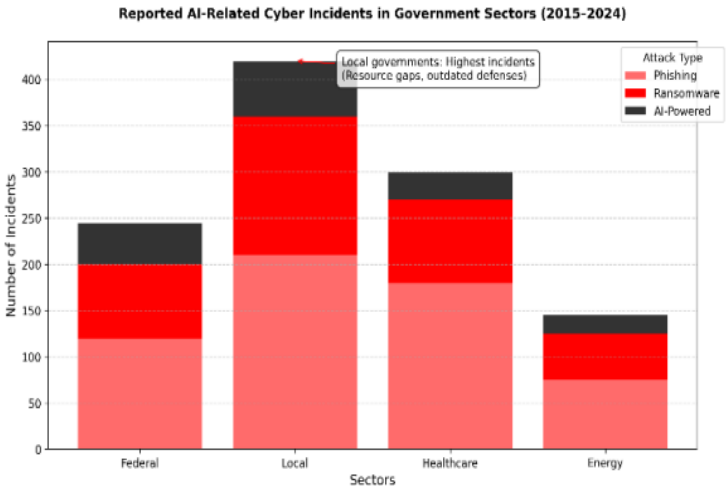

Figure 1. AI-Related Cyber Incidents in the Government Sector (2015–2024)

Due to the swift advancement of technology in high-hazard Cyber-Physical Systems (CPS), there exist multiple possible study routes concerning the governance of their development, operation, maintenance, and eventual disposal. The integration of cyber components into existing physical systems for both critical and non-critical functions is resulting in a proportional increase in the number of CPS. The Cisco Annual Internet Report (2018–2023), a public White Paper reveals a rise in machine-to-machine (M2M) connectivity from 2018 to 2023 (CISCO, 2020). M2M connections are taken as a representation of CPS that are connected to the internet, and show sustained growth in CPS volume not actual CPS volume. The data show that M2M connection growth increased from 33% to 50% of overall internet connectivity in the same period, indicating a greater growth in CPS compared to traditional IT systems/devices.

Municipal government agencies feel increasing pressure from threat actors due to the effects of digitalization, legacy infrastructures, and lack of institutional resources. Traditional approaches to threat modelling were often unable to truly assess or recognize security-dominant or AI-related threats, resulting in high levels of false positives, or rule-based deficiencies. The absence of threat modelling approaches combining AI and compliance with governing: security, legal, and regulatory requirements creates vulnerabilities and prevents the proper governance and regulatory approaches for cybersecurity in local government service delivery. The goal of the paper is to develop an AI-enabled threat modelling framework that uses Generative AI to generate assessments of secure-dominant threats, limit false positives, and create threats and mitigants on its own but all while connecting to governing compliance in cybersecurity policy, legal compliance in security, and regulatory compliance in a municipal government service delivery context.

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

LITERATURE REVIEW

Shaukat et al. (2020) highlighted that the accelerated digitization of society has increased risk exposure to cyberattacks, thus creating cybersecurity as a core building block of a new digital world. The review highlighted how machine learning (ML) techniques dealing with fraud/ intrusion/ spam/ virus detection are advancing - detection of threats. Nevertheless, it also revealed ongoing problems such as false positives; limited datasets; issues in deployment; which only shows the need for more stretchable AI models.

Van Landuyt and Joosen (2021) traced the history of security threat modelling of software systems, citing the lack of traditional tools such as Data Flow Diagrams (DFDs). Their results indicated that there were inconsistencies in how assumptions were recorded and understood across STRIDE models, calling for more systematic, context-aware approaches that integrate dynamic attacker and trust models in order to improve analytical robustness and consistency.

Mauri and Damiani (2022) expanded on this area by presenting STRIDE-AI, a conceptual asset-based approach meant for AI-ML systems. Their study closed the security gap during the ML lifecycle through the "Failure Mode and Effects Analysis (FMEA)" and "Microsoft' STRIDE'' framework and provided practitioners with a deterministic manner to be on watch for the ML specific risk so that effective protection AI asset.

Amoo et al. (2024) studied the universal implications of the General Data Protection Regulation (GDPR) for cybersecurity and data privacy practices. Their comparison of the United States and Europe noted the transformative implications of GDPR for its mandates of transparency, accountability, and proactivity, raising an important discussion on its increased weight of US federal privacy legislation. The study reinforced the territorial impact of GDPR and position as central to the formation of global cybersecurity governance.

Adesokan-Imran (2025) also reinforced the importance of cybersecurity governance as essential for a nation's resilience. By using statistics from CISA, GAO, and WEA, proposed data harmonized frameworks (such as NIST and ISO 27001) were found to reduce cybertacks over 75%. Unfortunately, imbalances in regulations, funding, and capacity were still concerns. The study advocacy data harmonized regulations with regular audits and increased awareness.

The reviewed literature illustrates substantial progress in employing AI and machine learning for uses in cybersecurity; however, significant gaps remain to be filled. While Shaukat et al. (2020) indicated the merits of machine learning approaches regarding threat identification, their work fails to acknowledge how these models should be entered into the notions of governance and regulation to ensure compliance and accountability. Van Landuyt and Joosen (2021) discovered limitations in existing threat modelling methods, but they restricted their discussion of governance and policy to the issue of technicality. Mauri and Damiani (2022) describe STRIDE-AI as a framework for AI-ML ecosystems based on an asset-centric view; however, it fails to focus on the unique problems of public sector organisations that are bound by compliance with standards and regulations. Therefore, there exists a significant gap in research in addressing a threat modelling framework that uses AI and machine learning

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

specifically for local governments, that not only improves the detection of cyber threats, but inserts compliance, governance and accountability, and transparency in the security space.

This research presents an original and cohesive approach to AI threat modelling that fits with the rapid advancements in governance. The study synthesizes methodologies associated with technological detection efficacy and enforcement regimes to contribute to a qualitative, AI-supported threat modelling methodology that reduces false positives and upholds regulatory regimes. The study's practice utilizes Generative AI methods to self-describe threats and subsequently establish mitigation actions without necessarily formally inciting explainability and transparency in decision-making. The approach pairs AI threat modelling with legal and governance principles to propose a framework to facilitate ethical AI regimes, without precluding accountability, and ahead-of-compliance. The research is framed against the backdrop of supporting cybersecurity for local governments, an under-explored, high-risk sector undergoing insulin transformation without appropriate levels of AI-supported and protective provisions.

RESEARCH METHODOLOGY

Research Design

The article proposes a theoretical synthesis of AI method with governance and compliance ideals. Rather than relying on empirical datasets, the article incorporates previous research findings and regulations on governance and compliance such as GDPR, NIST, and ISO 27001, to propose a conceptual framework that visually represents the functioning of AI-enabled threat modelling in a compliance- and transparency-governed system. The architecture allows a chance to examine a possibility for future implementation, whilst proposing an organized structure for future verification by empiricist methods. The research design theorizes a future-oriented possibility for local governments to enhance cybersecurity resilience through AI-enabled policy mechanisms while integrating AI-based threat modelling with legal culpability, regulatory compliance, and ethical governance ideals.

Data Collection

This research work is based exclusively on secondary data obtained from many reliable sources, including policy papers, cybersecurity guidelines, government-kind reports, and past academic research regarding AI, governance, and cybersecurity compliance. All of these sources provide an extensive theoretical basis to construct the conceptual framework of AI-based threat modelling for local government operations.

AI Centric Cybersecurity Policy Framework in Government

The rapid integration of AI into government operations today has both risks and opportunities, thus a cybersecurity policy framework based on artificial intelligence is needed to protect national security and support privacy values. Governments around the world appoint, institute security perspectives, and develop frameworks for managing risks associated with AI and legal and ethical requirements (Azmi et al., 2018).).

Identification of AI-Based Threat Modelling Principles

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cybersecurity standards and frameworks delineate structured mechanisms and methodologies for implementing security controls, risk management, and compliance within an AI system. These frameworks can be categorised into two primary domains: information security standards (e.g., ISO 27000 series or NIST SP 800) and governance standards (e.g., COBIT or NIST CSF). The integration of multiple standards is essential due to the complexity of AI systems, and governments typically provide only adequate security coverage for such systems.

Figure 2 shows the NIST Cybersecurity Framework that is widely adopted globally by organizations for cybersecurity risk management. The framework has six core functions - Govern, Identify, Protect, Detect, Respond, and Recover. Govern function ensures that organizations have clear visibility into the assets, and risks. Identify function is related to bookkeeping and tracking of assets in the organisations that are of interest to the attackers. Protect ensures that safeguards are implemented for the assets identified. Continuous monitoring for risks falls in the Detect function. Respond and Recover functions ensure quick response to cyberattacks and ensure availability to the users of the system.

Figure 2. Cybersecurity Framework (CSF) Core Functions for AI Risk Management[1]

AI-Specific Cybersecurity Challenges and Framework Adaptations

AI systems are susceptible to adversarial attacks, wherein fraudulent inputs mislead models (e.g., deepfake manipulation in governmental surveillance). A concise overview of several rules in the NIST SP 800-53 standard designed to safeguard the AI model from such risks is provided. AI systems in government must adhere to privacy legislation while safeguarding confidentiality (Cordero, 2021).

The ISO/IEC 27018 (cloud privacy) and ETSI EN 303 645 (IoT security) standards are pertinent to AI deployments that involve the processing of personal data. These ethical AI concepts are beneficial for adherence to the NIST Privacy Framework.

Figure 3 indicates the globally accepted governance standards for AI centric cybersecurity risk management. The three pillars indicated are ISO/IEC 27000 series, NIST frameworks, and

[1] https://csf.tools/reference/nist-cybersecurity-framework/v2-0/

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Industry specific standards. These standards enable organizations to build secure and regulatory friendly AI based solutions.

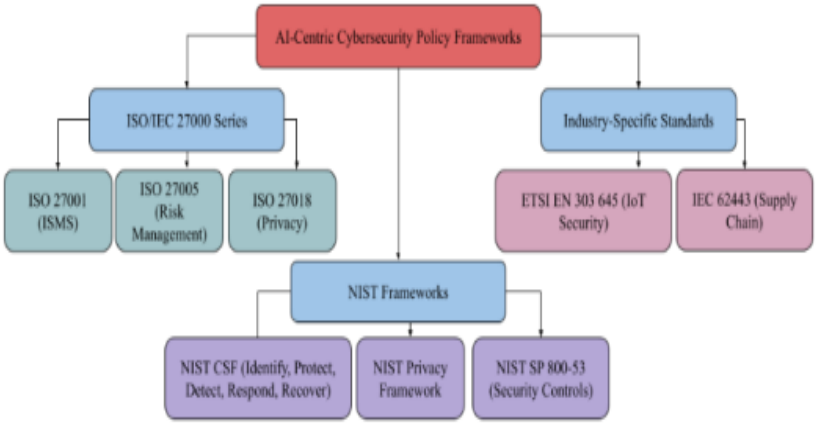

Figure 3. AI cybersecurity governance frameworks (Syafrizal et al., 2020)

Recommendations for AI-Focused Cybersecurity in Government Policy

India is developing and executing policy frameworks to regulate many facets of AI. Although complete legislation pertaining to AI are still developing, many initiatives and standards exist to direct the proper advancement and implementation of AI technology in India.

National Artificial Intelligence Strategy

In 2018, India launched its inclusive initiative for AI, termed #AIFORALL, as part of its first national AI plan. The strategy highlighted critical sectors for national priority in AI innovation and implementation, including healthcare, education, agriculture, smart cities, and transportation. Since then, numerous proposals specified in the strategy have been effectively executed, including the creation of high-quality datasets to facilitate research and innovation, along with the formulation of legal frameworks for data protection and cybersecurity[2].

Principles for Responsible AI

Formulated in February 2021, the Principles for Responsible AI constitutes the initial segment of an approach paper developed by NITI Aayog as a continuation of the national plan. It provides a basis for India to establish a professional and accountable AI ecosystem within industries. The ethical dimension noted in the paper has two dimensions: systemic and social (Karie et al., 2021). Systemic considerations address principles related to the decision and decision-making processes — that beneficiaries are engaged properly and are accountable for actions taken by the AI. Social considerations relate to the effects of automating a decision on job creation and work. The document delineates seven overarching principles for the responsible administration of AI systems: 1) Safety and reliability; 2) Inclusivity and non-

[2] https://www.psa.gov.in/mission/artificial-intelligence/34

Received: August 14, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

discrimination; 3) Equality; 4) Privacy and security; 5) Transparency; 6) Accountability; 7) Protection and reinforcement of positive human values[3].

Roadmap for AI Ecosystem

In March 2023, MeitY launched IndiaAI, the national program on artificial intelligence, designed as a comprehensive initiative to encompass all AI-related research and advancements.Employing a multistakeholder approach involving the government, academics, corporations, and start-ups, MeitY formed a taskforce tasked with devising a roadmap for the development, structure, and operation of IndiaAI[4].

Data Embassy Policy

In her budget address in February 2023, Finance Minister Nirmala Sitharaman declared that "for nations seeking digital continuity solutions, India will assist in establishing their Data Embassies in GIFT IFSC (Gujarat International Finance Tec-City International Financial Services Centre)[5]. The Minister of State for IT reported that the strategy will allow nations and corporations to establish "data embassies" in India, which will provide "diplomatic immunity" from local restrictions for both national and commercial digital data.

Policy Frameworks and Legal Considerations in AI Surveillance

The use of AI into surveillance systems has markedly improved national security capabilities, while also raising concerns about privacy and civil liberties. It is important to create broad-ranged policy frameworks and laws to find a suitable balance among competing interests. In order to balance these interests, complete policy frameworks should involve human-in-the-loop (HITL) controls for AI decisions for high-stakes situations (e.g., dangerous threat detection, biometrics-based identification) so that there is accountability and risk mitigation of bias (Leander, et al., 2019).

Additionally, governments ought to institutionalise a process of routine red-teaming finally, where ethical hackers will monitor AI systems for weaknesses, for discerning harsh critiques of blind spot issues in AI-directed definitions and to ultimately support transparency requirements. These practices may reinforce legal protections while better leveraging the security benefits of AI without compromising fundamental freedoms.

This paper assesses the efficacy of legal frameworks, looking at several important surveillance laws and consequential policies, including the GDPR, California Consumer Privacy Act (CCPA), as well as national and international policies addressing its surveillance tools. This paper explores issues around data privacy, consent, and accountability in AI-driven

[3] https://indiaai.gov.in/signin

[4] https://indiaai.gov.in/news/india-ai-will-become-a-global-innovation-and-research-brand-mos-rajeev-chandrasekhar

[5] https://www.indiabudget.gov.in/doc/budget_speech.pdf

Received: August 14, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

surveillance policy. This paper also discusses and reviews examples of the use of certain AI surveillance tools for social and state surveillance employed by governments and corporations to highlight some of the practical implications of current surveillance laws and demonstrate the identified gaps (Salem, et al. 2024).

According to the results of the study, the AI-based surveillance context is complex in which the benefits of AI-based surveillance for security and public safety are regularly challenged by ethical and legal concerns. A review of the literature and case studies show that, while carrying significant benefits to improved security, AI-based surveillance also poses serious risks to privacy and personal freedoms. For example, facial recognition is commonly used by police to identify and follow people in public spaces, but studies have shown that facial recognition systems often misidentify individuals in minorities, leading to wrongful arrests and exploiting social bias. Transfers of risk from AI-based surveillance to individuals state houses like the GDPR have tried to lessen these risks through data protection provisions about the use of AI-based surveillance. However, the results underscore that traditional regulatory frameworks have limitations in effectively addressing the embedded challenges to use of AI. As an example, the European GDPR relies on consent and transparency, however, it is unlikely there will be meaningful consent in situations where someone is surveilling another person in a public space. The vague wording in policies, and varied levels of enforcement, may also create scenarios where an organization finds a way out of situational definitions of privacy by obscuring meaning.

This research indicates that accountability plays an important role in the ethical use of AI surveillance. Accountability measures, such as having independent audits of AI algorithms or public accountability mechanisms, are required to address whether surveillance practices comply with ethical principles. The absence of accountability provisions in existing laws places organizations in a position to act as they feel they often have to when using these technologies. The findings indicate that if in place requirements for a clear accountability mechanism, but including if only for independent third-party auditing or public disclosures would help to address the ethical challenges to AI surveillance.

CONCLUSION

The research demonstrates that despite AI augmenting the range of potential threat detection in local government context, the true benefit comes when AI is integrated with legal, ethical and governance structures. Recent scholarship in addition to cross-national regulatory practices depict a substantial gap between technical detection technologies and regulatory-driven accountability structures that expose different municipal agents to compliance failures, as well as, governance blind spots. The theoretical AI-based threat modelling framework which is introduced here closes the gap between regulatory compliance, transparency, and dynamic significance of interpretability substantively integrating procedures into cybersecurity workflows that transition AI from a detection technology to a regulator-facilitating technology. The theoretical model presented here provides a backdrop for future empirical efforts and policy initiatives that will allow for local governments to transition to proactive governance-

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

compliant digital resilience models, as opposed to reactive approaches to cybersecurity compliance. This research attempts to create an operationally viable, yet ethically responsible public sector cybersecurity structure that allows AI creativity to be aligned to a continuum of governance integrity. Although the paper references AI policy initiatives of India, the proposed threat modeling architecture is designed using the globally accepted standards and is applicable to municipalities / local governments in any country or jurisdiction.

REFERENCES

1. Norris, D. F., & Mateczun, L. K. (2022). Cyberattacks on local governments 2020: Findings from a key informant survey. *Journal of Cyber Policy*, 7, 294–317. Retrieved from https://doi.org/10.1080/23738871.2022.2068287
2. Wolff, J., & Lehr, W. (2018). When cyber threats loom, what can state and local governments do? *Georgetown Journal of International Affairs*, 19, 67–75. Retrieved from https://gjia.georgetown.edu
3. Hatcher, W., Meares, W. L., & Heslen, J. (2020). The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. *Journal of Cyber Policy*, 5, 302–325. Retrieved from https://doi.org/10.1080/23738871.2020.1808795
4. Chaudhuri, A., & Bozkus Kahyaoglu, S. (2023). Cybersecurity assurance in smart cities: A risk management perspective. *EDPACS*, 67, 1–22. Retrieved from https://doi.org/10.1080/07366981.2023.2234595
5. Yigitcanlar, T., Agdas, D., & Degirmenci, K. (2023). Artificial intelligence in local governments: Perceptions of city managers on prospects, constraints and choices. *AI & Society*, 38, 1135–1150. Retrieved from https://doi.org/10.1007/s00146-022-01447-7
6. Yigitcanlar, T., Li, R. Y. M., Beeramoole, P. B., & Paz, A. (2023). Artificial intelligence in local government services: Public perceptions from Australia and Hong Kong. *Government Information Quarterly*, 40, 101833. Retrieved from https://doi.org/10.1016/j.giq.2023.101833
7. CISCO. (2020). *Cisco Annual Internet Report (2018–2023) Public White Paper.* Retrieved from https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html
8. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies.* Retrieved from https://doi.org/10.3390/en13174450
9. Mauri, L., & Damiani, E. (2022). Modeling threats to AI-ML systems using STRIDE. *Sensors (Basel, Switzerland)*, 22. Retrieved from https://doi.org/10.3390/s22166160
10. Van Landuyt, D., & Joosen, W. (2021). A descriptive study of assumptions in STRIDE security threat modeling. *Software and Systems Modeling*, 21, 2311–2328. Retrieved from https://doi.org/10.1007/s10270-021-00944-3

Received: August 14, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

11. Adesokan-Imran, T. (2025). The impact of cybersecurity governance on national security by strengthening critical infrastructure through IT auditing and risk management. *Asian Journal of Research in Computer Science.* Retrieved from https://doi.org/10.xxxx/ajrcs.2025
12. Amoo, O., Atadoga, A., Osasona, F., Abrahams, T., Ayinla, B., & Farayola, O. (2024). GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive.* Retrieved from https://doi.org/10.xxxx/ijsra.2024
13. Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security"*, 12, 417–432. Retrieved from https://doi.org/10.17762/ijcnis.v12i3.3575
14. Azmi, R., Tibben, W., & Win, K. (2018). Review of cybersecurity frameworks: Context and shared concepts. *Journal of Cyber Policy*, 3, 258–283. Retrieved from https://doi.org/10.1080/23738871.2018.1519030
15. Cordero, J. A. V. (2021). Les normes ISO/IEC com a mecanismes de responsabilitat proactiva en el Reglament General de Protecció de Dades. *IDP Revista de Internet, Derecho y Política*, 33, 7. Retrieved from https://raco.cat/index.php/IDP/article/view/380013
16. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*, 9, 121975–121995. Retrieved from https://doi.org/10.1109/ACCESS.2021.3109995
17. Leander, B., Causević, A., & Hansson, H. (2019, August 26). Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security*, Canterbury, UK. Association for Computing Machinery: New York, NY, USA. Retrieved from https://doi.org/10.1145/3339252.3340333
18. Salem, A., Azzam, S., Emam, O., & Abohany, A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data*, 11. Retrieved from https://doi.org/10.1186/s40537-024-00957-y.