World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

The role of cybersecurity regulation, policy, and compliance in strengthening IoT security and reducing consumer risks

Mildred Adwubi Bonsu [1], Derrick Atuobi Oware [2] and Alice Ama Donkor [2,*]

[1] *University at Albany, State University Of New York. USA.*
[2] *Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana.*

World Journal of Advanced Research and Reviews, 2025, 27(01), 2500-2507

Publication history: Received on 21 May 2025; revised on 28 June 2025; accepted on 30 June 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2508

Abstract

The proliferation of Internet of Things (IoT) devices has transformed modern living, but it has also introduced complex cybersecurity challenges and heightened consumer risks. This study critically examines the role of cybersecurity regulations, policy frameworks, and compliance mechanisms in enhancing IoT security and safeguarding consumers. Through a comprehensive analysis of regulatory landscapes, including global standards such as the NIST Cybersecurity Framework and the EU Cybersecurity Act, alongside sector-specific guidelines, the research evaluates the effectiveness of existing policies in mitigating threats inherent within the IoT landscape. The findings reveal that while fragmented regulations have left critical gaps, jurisdictions with cohesive, enforceable policies demonstrate significantly lower incidents of IoT breaches. Moreover, the research identifies that mandatory compliance measures and stringent enforcement drive better security practices among manufacturers and service providers. However, voluntary frameworks without clear accountability tend to result in inconsistent adoption. The study further uncovers that consumer education, combined with policy-backed device certification schemes, substantially reduces end-user vulnerability. This paper concludes that a cohesive approach of combining standardized regulations, proactive compliance incentives, and heightened consumer awareness markedly strengthens IoT security posture and mitigates consumer risks. These insights offer actionable recommendations for policymakers, industry leaders, and cybersecurity practitioners aiming to fortify the rapidly evolving IoT landscape.

Keywords: IoT Security; Cybersecurity Compliance; Regulatory Frameworks; Consumer Risk Mitigation

1. Introduction

Internet of Things (IoT) has transformed rapidly from a theoretical innovation to a ubiquitous reality in a very short period, becoming woven into modern daily life. IoT devices are now pervasive across industries and households, from empowering advanced automation in manufacturing and predictive maintenance in transportation networks to enabling smart energy management in homes and remote patient monitoring in healthcare settings. Early projections suggested that by 2025, it is estimated that more than 75 billion devices will be connected to the internet globally [1], marking an unparalleled expansion of digital interconnectivity, which has inevitably become our reality. While this burgeoning growth unlocks tremendous potential for efficiencies, convenience, and innovation, it also broadens the attack surface for malicious actors. Every connected device is a potential gateway for cyber breaches and in a hyper-connected environment, one vulnerable device can lead to widespread disruption. The effects of this transcend individual privacy breaches, as they can also have more serious consequences in national security and resilience in critical infrastructure [2,3].

* Corresponding author: Alice Ama Donkor

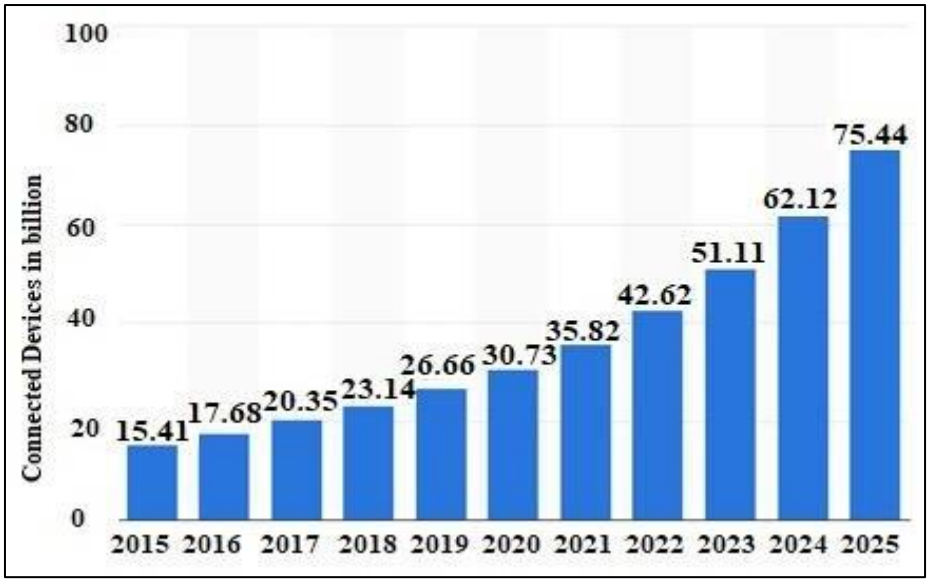

Figure 1 Internet of Things (IoT) connected devices from 2015 to 2025 (in billions) - (Statista, 2016)

Internet of Things is the interconnection of physical objects, ranging from wearable health trackers to industrial sensors embedded with computing capabilities that allow for data collection and exchange [4]. Though powerful, these devices rarely have robust security mechanisms, making them an attractive target for cybercriminals. On that account, cybersecurity regulation is a vital element in securing these digital environments. It includes an array of policies, regulations, and recommendations to secure digital infrastructures and sensitive data against the growing rates of cyber threats [5]. Compliance in this context refers to the adherence of organizations, manufacturers, and service providers to the specified cybersecurity requirements, limiting their exposure to legal lawsuits and reputation damage [6].

However, even though public understanding of the risks presented by IoT continues to grow, regulatory approaches are uneven and inconsistent across jurisdictions. Although frameworks like the European Union's General Data Protection Regulation (GDPR) and the U.S. National Institute of Standards and Technology (NIST) cybersecurity framework have offered helpful guidelines, the global landscape suffers from major differences in enforcement, scope, and applicability. These gaps lead to uncertainties for businesses that operate across borders and exacerbate vulnerabilities for consumers that rely on IoT technologies every day [7]. The risks for consumers are numerous, including personal privacy breaches, financial exploitation through devices that are not secured, and even physical harm as observed in incidents of a compromised medical device or autonomous system [8].

With rapidly evolving threats surrounding IoT ecosystems, this research aims to critically analyze the roles of cybersecurity regulations, policy frameworks, and compliance mechanisms in improving IoT security while reducing risks to consumers. The research studies the effectiveness of current regulatory approaches in detail, leveraging a comprehensive review of existing literature, and outlines their inherent limitations as well as areas for significant improvement. In doing so, the study maps out the most prevalent regulatory frameworks that currently govern the security of IoT, outlining the way these systems are designed in practice to protect users and their data in the real world. Moreover, it assesses how policy and compliance mechanisms contribute to mitigating consumer risks, ranging from data breaches and privacy violations to more aggravated threats targeted at critical infrastructure. However, focus is placed on identifying the persistent gaps and challenges that continue to impede efforts towards cohesive global governance in IoT cybersecurity. With this nuanced exploration, the paper provides insights of practical relevance for immediate practical utility for decision-makers shaping future regulations, practitioners who seek to improve security standards, and academics who are interested in advancing academic discussions in this significant area.

2. Overview Of Iot Vulnerabilities

Due to the rapid proliferation of IoT devices, security vulnerabilities have significantly expanded, increasing the digital attack surface and exposing both consumers and organizations to a range of security vulnerabilities. Most IoT devices are designed with minimal secure protocols and often lack essential safeguards such as encryption, secure authentication, and timely firmware updates [9]. With this security gap, devices are left vulnerable to breaches of privacy, unauthorized access to data, and exploitation by malicious individuals. The infamous Mirai botnet attack in

2016, which exploited thousands of vulnerable IoT devices for global-scale distributed denial-of-service (DDoS) attacks, clearly demonstrates the devastating consequences of unsecured IoT devices [10]. This unprecedented cyber-attack was targeted at Dyn, one of the leading providers of domain name system (DNS) services, effectively overwhelming its servers with malicious traffic and rendering some major websites unreachable across Europe and the United States. Platforms such as Reddit, Twitter, CNN, the Guardian, and Netflix experienced prolonged outages for hours, indicating the vast disruption that can result from compromised IoT systems. The Mirai botnet operated by infecting connected devices, including poorly secured consumer products such as webcams and home routers and marshaling them into a coordinated network of malicious traffic generators. The efficiency and scale of this attack revealed the vulnerabilities inherent in everyday IoT devices and the potential for these weaknesses to be exploited in orchestrating attacks of such magnitude [11].

Moreover, the problem of insecure default configurations still remains, with manufacturers sometimes prioritizing ease of deployment over hardening security of devices [12]. In smart home environments, for instance, weak or unchanged default passwords have, more often than not, allowed perpetrators to breach private networks. Attacks on a large scale are not limited to the consumer space either, and the risks to industrial IoT deployments keep growing. Recent studies have acknowledged the vulnerability of industrial control systems (ICS) to advanced cyber intrusions that threaten essential and critical infrastructure services and operations. In IoT environments, the convergence of both physical and digital threats heightens their security concerns, making the security of IoT devices an urgent global priority [13].

3. Role of Regulations Globally

Recognizing the scale of IoT security challenges, policymakers across the globe have enacted diverse regulatory frameworks to strengthen defenses. For example, in Europe, the General Data Protection Regulation (GDPR) places strict obligations on data controllers and processors, requiring robust protection of data and imposing severe penalties for non-compliance [14]. While GDPR is not IoT-specific, its broad applicability ensures that IoT devices that process personal data fall within its scope and promote greater accountability.

In the United States, National Institute of Standards and Technology (NIST) created the NIST Cybersecurity Framework, which offers voluntary guidance to help organizations understand and manage their cybersecurity risk, including those associated with IoT [15]. In addition to that, the IoT Cybersecurity Improvement Act of 2020 focuses on the security of IoT devices owned or controlled by the federal government, mandating compliance with standards developed by NIST [16]. This collection of regulatory instruments highlights a recognition that IoT Security is a matter of national and economic importance.

Although these advances have been made, the global regulatory landscape remains fragmented. In some countries, especially in the developing parts of the world, comprehensive cybersecurity legislation is currently lacking, ultimately leaving consumers vulnerable to unmitigated threats [17]. Such constraints hamper coordinated responses to cyber threats that extend national borders.

4. Compliance and Enforcement

Although the existence of regulatory frameworks is paramount, their effectiveness largely hinges upon industry compliance and the robustness of enforcement strategies. Compliance enables organizations to adhere to established cybersecurity standards, which helps lower vulnerabilities within the IoT landscape [5]. However, studies indicate that compliance levels differ widely across sectors and regions, and are often influenced by organizational culture, available resources, and the perception of severity for the penalty for non-compliance.

Enforcement continues to be a significant challenge. Even in jurisdictions having well-defined regulations, inadequate enforcement resources and overlapping geographic and jurisdictional limitations can hinder their effective oversight. Without strict enforcement, regulations risk becoming more symbolic rather than a substantive deterrent. Moreover, the accelerating rate of technological innovation in the IoT space surpasses the capacity of regulators to keep standards current, leading to a persistent lag between the emergence of new threats and regulatory action.

5. Consumer Risks and Impacts

Consumers are faced with multifaceted risks stemming from inadequate IoT security.

Inadequate IoT security poses complex risks to consumers ranging from privacy violations to serious financial loss. Data breaches stemming from compromised IoT devices can result in exposure of sensitive personal information, identity theft, fraud, and reputational damage [19]. According to a survey from PwC, nearly 60% of consumers are worried about how companies use and protect their data, indicating widespread apprehension.

Outside of data privacy, the harvesting of personal information via IoT devices can also enable targeted scams and exploitation. In extreme cases, poorly secured IoT devices in medical contexts like pacemakers or insulin pumps may create life-threatening risks when manipulated for malicious purposes [20]. In addition, consumers are also faced with the need to pay for repairs, data recovery, and identity protection services, which all contribute to the financial impact [21]. All of these risks cumulatively erode consumer trust, which is crucial for the continued adoption and development of IoT technologies.

5.1. Existing Gaps

Despite the growing body of research literature and policies, the global approach to IoT cybersecurity still suffers from major gaps. At the outset, one of the key problems is the highly fragmented and disparate nature of international regulations, which makes it challenging to define universal security baselines [17]. Though GDPR, the NIST-based framework, and similar initiatives may provide some additional regional guidance, the absence of any harmonized ethical global baseline means IoT devices remain vulnerable as they pass from one jurisdiction into another.

Moreover, the sociolegal aspects of cybersecurity governance have often been neglected in existing literature, focusing primarily on technical solutions [2]. Hence, this calls for more integrative approaches considering human factors, behavioral compliance, policy enforcement, and technical safeguards. As IoT technologies continue to advance, so do the tactics employ by cyber adversaries. This dynamic threat landscape necessitates continuous updates to compliance and regulatory frameworks, which is a demand that current legislative processes are barely keeping up.

5.2. Insights from Existing Frameworks

The emerging IoT security landscape has prompted significant regulatory responses, most notably in regions like the EU and the United States. Amongst the most impactful of these frameworks is the EU's General Data Protection Regulation (GDPR), which, while primarily concerned with data protection and privacy, has tremendous implications for securing IoT. GDPR mandates data protection by design and by default, which compels manufacturers and service providers of IoT to include security features and measures in their product development [14]. IoT devices that gather personal information, for example, need to ensure secure encryption, secure data storage, and provide users with clear information about how their data is being used. In addition, GDPR imposes stringent breach notification requirements, which demand organizations to notify of a data breach within 72 hours, thereby encouraging more robust internal security policies [22].

In contrast, the U.S. takes a more fragmented, sectoral approach, with some of the best-known efforts coming from the National Institute of Standards and Technology (NIST). "Considerations for Managing Internet of Things Cybersecurity and Privacy Risks" (NISTIR 8228) provides a voluntary framework that guides the mitigation of cybersecurity and privacy risks associated with the Internet of Things (IoT). It helps organizations and manufacturers to protect device security, protect data security, and protect individual privacy from cyber threats [15]. Although not legally binding, NIST guidelines form the bedrock of industry best practices, informing both private sector practices and public policy. On the contrary, NIST does not have the same legal implications as GDPR and instead relies on stakeholder adoption and market incentives to ensure compliance, which can lead to inconsistent implementation across different industries [23].

A comparative analysis reveals a transatlantic divergence of regulatory philosophy between GDPR and NIST. Unlike GDPR, which imposes strict requirements and punitive consequences, NIST's framework provides flexible, risk-based guidance. Such disparity underlines the difficulties of establishing unified global security standards for IoT security, as regional priorities and legislative cultures shape the landscape of compliance expectations.

6. Compliance effectiveness

Effective enforcement of cybersecurity legislation is important in reducing risks associated with IoT. In the EU, GDPR's strict rules have resulted in substantial fines for companies that do not follow privacy standards, underscoring the need for proactive security strategies. For example, in 2021, Amazon Europe faced a fine of €746 million, which is the highest fine ever issued for GDPR violations, which sent a strong message to the technology industry, including IoT manufacturers, about the potential financial impact of non-compliance [24].

In the U.S., for instance, while NIST's guidance framework is completely voluntary, federal law, such as the IoT Cybersecurity Improvement Act of 2020, mandates minimum security standards for IoT devices that are procured by the government [25]. This legal requirement has, indirectly, also had a tremendous effect on commercial markets, significantly raising the baseline of security expectations. By setting procurement standards, the government can use its purchasing power to incentivize a broader level of compliance and encourage private enterprises to implement higher cybersecurity standards voluntarily.

Furthermore, industry-driven compliance programs like certification schemes and security seals for IoT devices become particularly relevant when it comes to trustworthiness, as they assure consumers and establish trust. These initiatives, although not legally mandated, create markets incentives for manufacturers and developers of industrial IoT to prioritize cybersecurity, illustrating the useful potential of a combination of regulatory enforcement and voluntary compliance, which can yield positive outcomes [26].

6.1. Identified Challenges

Despite major advancements, there are still some persisting difficulties in enhancing the security level in the IoT ecosystem. One is the rapid pace of IoT technology itself. New devices and even new applications emerge constantly, and regulatory frameworks struggle to keep pace. Many IoT devices are designed for low cost and mass deployment at the expense of robust security features [9]. Speed to enter the market often trumps rigorous security testing during development, leaving security vulnerabilities unaddressed after deployment.

In addition, these risks are compounded by the existence of regulatory lag. Legislative processes take longer than technological innovation, and that results in outdated laws that can't keep pace with the emerging threats. While the IoT Cybersecurity Improvement Act sets baseline standards for federal devices, it does not cover the extensive consumer IoT market domain, thus leaving a significant portion of the IoT ecosystem under-regulated [7].

A complication comes from the fragmented nature of global cybersecurity governance. In the absence of unified international standards, manufacturers are subjected to a patchwork of inconsistent jurisdictional regulations, raising the complexities and allowing for enforcement gaps. Countries with weaker regulatory environments could easily become havens for substandard devices, which can still infiltrate global markets and drive widespread vulnerabilities [27].

6.2. Case Illustrations

Real-life incidents clearly demonstrate the consequences of IoT security lapses. The health industry, for instance, has become increasingly targeted by cybercriminals because of its reliance on connected medical devices and sensitive patient data. In 2021, the ransomware incident on the Ireland Health Service Executive (HSE) seriously affected the healthcare services across the country and served as a wake-up call for security in healthcare IoT environments [28]. The attackers exploited weaknesses in remote access systems, freezing diagnostic services and compromising patient information.

Likewise, smart home ecosystems present growing vulnerabilities. Devices like smart locks, cameras, and voice assistants mostly operate with minimal security, which makes them attractive targets for attackers. A study by Fernandes et al. [29] illustrated how adversaries may exploit and compromise poorly secured smart home hubs and gain control over connected devices. Comparing the EU and US responses to these challenges further emphasizes their differing strategies. Privacy and mandatory security obligations under GDPR by the EU provide stronger legal recourse for consumers affected by IoT breaches. The US, on the other hand, policies have traditionally placed more reliance on market-driven solutions and post-incident enforcement, although recent legislative developments suggest a shift towards more proactive regulation [30].

7. Discussion

The evolution of IoT threats, along with existing national and regional regulatory efforts to address them, reveals that while certain frameworks have become popular, they fall short in creating a cohesive global defense against consumer-facing risks. One of the strongest insights from this study is the understanding that the lack of synchronized international regulations should not only be thought of merely as a bureaucratic hindrance; rather, it directly enables the proliferation of risk across the IoT landscape [31]. Variations in definitions, levels of enforcement, and expectations of security across jurisdictions leave important blind spots that malicious actors are actively exploiting, especially in low-regulation or under-resourced regions [32]. Beyond technology, these gaps are legal and procedural, allowing a

worldwide circulation of insecure devices that would fail even basic compliance checks in more strictly regulated markets [19].

Although frameworks, such as GDPR and NIST, have contributed as pressure points for companies to adopt higher standards, these frameworks are often predicated upon a level of infrastructure, enforcement capability, and political will that some countries do not possess [27, 15]. This becomes problematic due to globalized manufacturing and cloud infrastructure. For example, an IoT device that is produced in a jurisdiction with less stringent data protection legislation, is still capable of entering and operating in a more restrictive region with little impedance, leaving the consumer in the latter open to vulnerabilities created by regulatory shortfalls in another region [33]. Despite well-crafted laws in certain countries, without an enforcement mechanism that can reach across borders, such vulnerabilities persist [31].

In addition, the compliance culture itself is mainly reactive than adaptive. Organizations tend to adopt a "checklist" approach to compliance, aiming to meet the minimum legal requirements but fail to incorporate a culture of proactive cybersecurity [34]. This technique becomes particularly dangerous with IoT context as rapid device lifecycles, lack of long-term support, and inconsistent firmware updates provide opportunities for dormant threats to come up with time [35]. Given the rapidly changing threat landscape, it calls for compliance models that are not just based on current risks but are agile enough to anticipate evolving vectors, which is a gap identified in existing research [19].

This uneven adoption of security standards is partially due to a struggle to balance the promotion of innovation and enforcing restrictions. To attract manufacturing and tech evolution, countries that compete in the IoT race may choose looser regulations; inadvertently creating ecosystems where security is sacrificed in favor of speed and cost efficiency [31]. This economic reality makes the idea of global standardization complicated, as balancing sovereignty with collective cybersecurity responsibility will be required [32].

Additionally, large IoT platform providers and manufacturers have a high degree of control over device ecosystems. Their lobbying efforts and standard-setting roles, often more influential than governmental bodies, can either strengthen or weaken regulatory initiatives [34]. The role and potential of industry consortia like the Internet of Things Security Foundation [36] or alliances like the Connectivity Standards Alliance [37] is worthy of deeper investigations, as they may provide conduits to pragmatic, industry-led regulations and fill global governance gaps.

8. Conclusion

This research explored the conditional influences of cybersecurity regulation, policy, and compliance mechanisms on the security posture of Internet of Things (IoT) systems and how they enable the protection of consumers. The study found that against the backdrop of rapid adoption of IoT devices and increasing reliance on such connected technologies by consumers, gaps remain between existing regulatory efforts, manufacturers' responsibilities, and consumer protection in an increasingly interconnected digital ecosystem. A more coherent and collaborative international framework is essential, to ensure manufacturers are accountable regardless of where they operate, and also to ensure consumers benefit from consistent security standards no matter their geography. Additionally, this research also illuminates the gap between compliance and actual security outcomes, with products able to meet the letter of regulatory standards but still falling victim to threats in practice, especially when security updates are not mandated in post-market or when users are not provided with clear guidance on how to use the products securely. In conclusion, this research addresses the challenges posed by IoT technologies and lays the groundwork for a sustainable IoT ecosystem by promoting the need for a proactive regulatory model over a reactive one, while preserving a self-sustaining, decentralized ecosystem. It underscores the urgent need for enhanced accountability, transparency, and international cooperation if the trust of consumers in IoT is to be preserved and strengthened.

Recommendations

Institutions, like the Organization for Economic Co-operation and Development (OECD), International Telecommunication Union (ITU) or even specialized multi-stakeholder alliances could help facilitate this kind of transnational collaboration and enforcement directly. Manufacturers also need to transition from a reactive to proactive security posture, embedding privacy and resilience into every aspect of their product lifecycle. This means creating IoT devices that are built with robust encryption, security updates, and strict data handling protocols in mind right from the inception. Governments can support the acceleration of this transition by incentivizing compliance with tax benefits or certification schemes and penalizing negligent conduct. In addition to governmental and industry action, academia and cybersecurity researchers should prioritize future studies that examine adaptive governance models, either via regulatory sandboxes or international testbeds. These studies can provide empirical evidence of which combination of

innovation, regulation, and enforcement provides the most secure results, particularly within emerging economies where IoT adoption is rapidly increasing, but policy support is still developing.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Statista, 2016. Number of connected devices worldwide 2015–2025. Available at: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] Conti, M., Dehghantanha, A., Franke, K. & Watson, S., 2018. Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, pp.544-546. doi: 10.1016/j.future.2017.07.060

[3] Jurcut, A., Niculcea, T., Ranaweera, P. and Le-Khac, N.A., 2020. Security considerations for Internet of Things: A survey. SN Computer Science, 1, pp.1-19.

[4] Asplund, M. & Nadjm-Tehrani, S., 2016. Attitudes and Perceptions of IoT Security in Critical Societal Services. IEEE Access, 4, pp.2130-2138. doi: 10.1109/ACCESS.2016.2560919

[5] De Bruijn, H. & Janssen, M., 2017. Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies. Government Information Quarterly, 34(1), pp.1-7.

[6] Trend Micro. (2025) What is Cyber Security Compliance? Available at: https://www.trendmicro.com/en_no/what-is/governance-risk-management-and-compliance-grc/cyber-security-compliance.html

[7] Roman, R., Zhou, J. & Lopez, J., 2013. On the Features and Challenges of Security and Privacy in Distributed Internet of Things. Computer Networks, 57(10), pp.2266-2279. doi: 10.1016/j.comnet.2012.12.018

[8] Haney, J. M., Furman, S. M., & Acar, Y. (2020). Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. International Conference on Human-Computer Interaction, Copenhagen. National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=929479

[9] Sicari, S., Rizzardi, A., Grieco, L. & Coen-Porisini, A., 2015. Security, Privacy and Trust in Internet of Things: The Road Ahead. Computer Networks, 76, pp.146-164. doi: 10.1016/j.comnet.2014.11.008

[10] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80–84.

[11] Woolf, N. (2016). DDoS attack that disrupted internet was largest of its kind in history, experts say. The Guardian. Available at: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[12] Fernandes, E., Rahmati, A., & Prakash, A. (2017). Security implications of permission models in smart-home platforms. IEEE Security & Privacy, 15(2), 24–30.

[13] Cybersecurity and Infrastructure Security Agency. (2021). Cybersecurity and physical security convergence action guide. U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide

[14] Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.

[15] NIST. (2020). Considerations for Managing IoT Cybersecurity and Privacy Risks (NISTIR 8228). National Institute of Standards and Technology.

[16] Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). Foundational Cybersecurity Activities for IoT Device Manufacturers. NISTIR 8259. National Institute of Standards and Technology.

[17] Khan, N.A., Awang, A. and Karim, S.A.A., 2022. Security in Internet of Things: A review. IEEE access, 10, pp.104649-104670.

[18] Transforma Insights. (n.d.). Position paper: Meeting the increasing regulatory challenge in IoT. https://transformainsights.com/research/reports/position-paper-meeting-regulatory-challenge-iot

[19] Roman, R., Najera, P. and Lopez, J. (2011) Securing the Internet of Things. IEEE Computer, 44, 51-58. https://doi.org/10.1109/MC.2011.291

[20] Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., & Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. IEEE Symposium on Security and Privacy, 129–142. https://doi.org/10.1109/SP.2008.31

[21] Harkai, A., & Ciurea, C. E. (2024). Economic impact of IoT and conventional data breaches: Cost analysis and statistical trends. Control and Cybernetics, 53(2), 385–404. https://doi.org/10.2478/candc-2024-0017

[22] European Union Agency for Cybersecurity (ENISA) (2023) ENISA Threat Landscape 2023: July 2022 to June 2023. October 2023. Available at: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

[23] Delgado, M.F., Esenarro, D., Regalado, F.F.J. and Reátegui, M.D., 2021. Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. 3 c TIC: cuadernos de desarrollo aplicados a las TIC, 10(2), pp.123-141.

[24] Greenleaf, G. (2023) Global Data Privacy Laws: EU Leads US and the Rest of the World in Enforcement by Penalties. Privacy Laws & Business International Report, (181), pp. 24–29. UNSW Law Research Paper No. 23-47. Available at: https://ssrn.com/abstract=4409491

[25] U.S. Congress (2020) IoT Cybersecurity Improvement Act of 2020, Public Law No: 116-207. Available at: https://www.congress.gov/bill/116th-congress/house-bill/1668

[26] Khurshid, A., Alsaaidi, R., Aslam, M. and Raza, S. (2022) 'EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme', IEEE Access, 10, pp. 129932–129948. doi: 10.1109/ACCESS.2022.3225973.

[27] ENISA, 2021. Guidelines for Securing the Internet of Things. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[28] HSE NQPSD (2022) A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare ICT failure. Dublin: National Quality and Patient Safety Directorate (NQPSD) of the Chief Clinical Officers Office, Health Service Executive

[29] Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications. IEEE Security & Privacy.

[30] Macnish, K. and van der Ham, J. (2020) 'Ethics in cybersecurity research and practice', Technology in Society, 63, 101382. doi: 10.1016/j.techsoc.2020.101382.

[31] Chiara, P. (2022). The IoT and the new EU cybersecurity regulatory landscape. International Review of Law, Computers & Technology. 36. 1-20. 10.1080/13600869.2022.2060468.

[32] Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30.

[33] Yu, H. (2018) GDPR isn't enough to protect us in an age of smart algorithms, 31 May. Available at: https://www.howardyu.org/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms/

[34] Restuccia, F., D'oro, S. and Melodia, T., 2018. Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet of Things Journal, 5(6), pp.4829-4842.

[35] Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65–88.

[36] Internet of Things Security Foundation (IoTSF). (2021). IoT Security Compliance Framework Release 3.0. Available at: https://www.iotsecurityfoundation.org

[37] Connectivity Standards Alliance (CSA). (2023). Building the Foundation & Future of the IoT - Annual Report. Available at: https://csa-iot.org/wp-content/uploads/2024/05/2023-Connectivity-Standards-Alliance-Annual-Report.pdf