IJARSCT

ISSN (Online) 2581-9429

IJARSCT

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 2, May 2024

IoT Security Challenges and Solutions for Data at Rest: A Systematic Literature Review

Chisomo Tolani[1] and Dr. Jyoti Pareek[2]
Research Scholar, Department of Computer Science[1]
Professor and Head of Department, Department of Computer Science[2]
Gujarat University, Ahmedabad, India

Abstract: *The rapid expansion of the Internet of Things (IoT) has significantly transformed both consumer and industrial domains, driving the urgent need for robust security measures to protect data at rest. SLR investigates into the challenges associated with securing IoT devices and data, exploring the limitations of existing security frameworks and the intricate requirements imposed by global data protection regulations such as GDPR. The researcher review current approaches, including privacy-by-design principles and the deployment of symmetrical data protection frameworks, as highlighted in recent studies. Through a comprehensive analysis of literature and existing technologies, we identify critical gaps in the protection strategies and propose enhanced methods for ensuring data security and privacy in IoT systems. The findings emphasize the role of developers in integrating privacy considerations early in the development process and the impact of regulatory complexities on the practical implementation of data protection measures. Furthermore, the paper evaluates innovative security solutions, such as full stack security architectures and adversarial training models, assessing their effectiveness in real-world applications. This study aims to provide a deeper understanding of the IoT security landscape and to suggest actionable strategies for improving data protection practices across the IoT ecosystem.*

Keywords: Internet of Things, data security, GDPR, privacy-by-design

I. INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) has dramatically transformed everyday computing and communication landscapes. With applications ranging from smart automobiles and smart cities to smart grids, IoT technologies are redefining human interactions with digital and physical environments. Despite these advancements, the integration of IoT systems raises substantial concerns regarding data security and privacy, necessitating the implementation of stringent privacy-preserving measures and robust security frameworks. The General Data Protection Regulation (GDPR) and privacy-by-design principles have been pivotal in addressing these concerns; however, their application in the IoT context remains complex and fraught with challenges (van Mill &Quintais, 2022). This paper aims to explore the current state of IoT security, focusing on the protection of data at rest, the identification of potential threats, and the evaluation of existing data protection frameworks and their limitations.

II. LITERATURE REVIEW

Privacy and Security in IoT Development: The complexity of IoT systems has necessitated a shift in how privacy and security are integrated into technology development. Kühtreiber et al. (2022) emphasize the inadequacies in current frameworks and tools for IoT privacy engineering, highlighting the need for more research into developer-friendly privacy solutions. IoT developers, often not viewing privacy as a primary concern, must be actively involved in creating these solutions to ensure comprehensive privacy protection. This involvement is critical as IoT devices become increasingly prevalent in sensitive environments, where data privacy cannot be an afterthought.

Data Protection Challenges and Frameworks: In addressing the specific needs of IoT devices, Abdulghani et al. (2019) identify several challenges in deploying traditional internet security solutions, largely due to the limited capabilities of IoT devices and the lack of universally accepted security standards. They propose a symmetrical framework that integrates user-generated data protection, aiming to enhance IoT security from a design perspective.

DOI: 10.48175/IJARSCT-18175

However, the framework also reveals significant gaps that necessitate further investigation into effective data protection methodologies.

Innovative Solutions and Evaluations: The development of new solutions to address the privacy and security concerns in IoT has led to significant innovations in both hardware and software aspects of IoT networks. For instance, Badii et al. (2020) discuss the Snap4City architecture, which incorporates full stack security encompassing cloud applications, edge computing, IoT devices, data analytics, and dashboarding. This solution was validated in large-scale urban deployments, thereby confirming its efficacy in real-world settings. Furthermore, Zhang et al. (2022) introduce a novel data protection technique utilizing data disruption and adversarial training to enhance security in collaborative edge computing (CEC), demonstrating improved performance metrics in robustness and accuracy.

Regulatory Challenges and Market Impacts: The intricacies of complying with GDPR in IoT implementations have been a point of contention, as noted by van Mill &Quintais (2022), who argue that the regulation's complexity makes it challenging to identify controllers and joint controllers. Additionally, the rise of IoT coupled with artificial intelligence has expanded the market for smart devices, such as smart speakers. Liu et al. (2022) examine the implications of China's Personal Information Protection Law (PIPL) on this market, offering insights into how regulatory frameworks can shape industry practices and consumer perceptions.

While IoT technologies bring remarkable benefits and conveniences, they also introduce significant privacy and security challenges that must be addressed through continued research, innovative solutions, and adaptive regulatory frameworks. This review sets the stage for discussing specific security objectives for IoT data at rest, exploring both the technological frameworks and the legal and ethical considerations impacting their development and deployment.

Objective: Examine IoT security for data at rest, evaluate frameworks, and propose solutions for identified gaps.

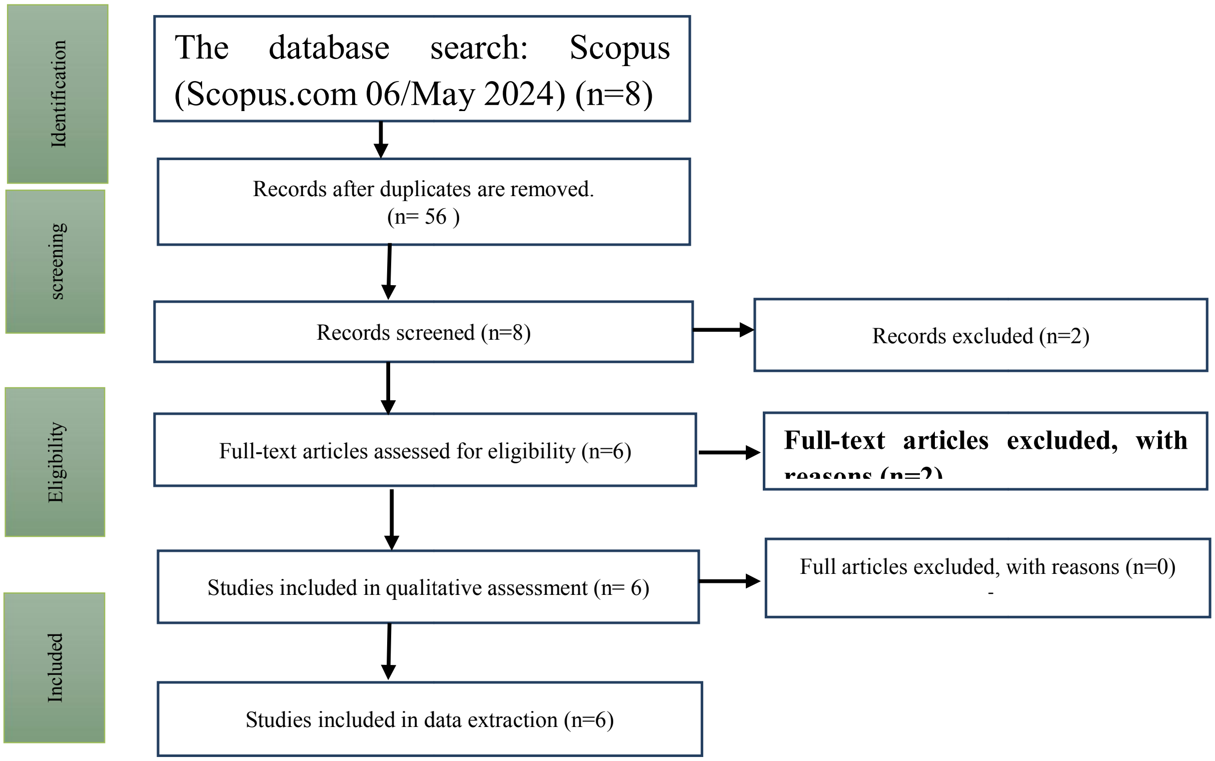
III. METHODOLOGY

The methodology described for the Systematic Literature Review (SLR) focuses on analyzing recent trends within the field of computer science, specifically relating to the Internet of Things (IoT), data privacy, and associated legal regulations. Documents were retrieved on 6 May 2024, and the review includes articles published between 2019 and 2024, ensuring that the literature examined is current and relevant. The scope of this review is confined to eight peer-reviewed articles, highlighting a precise and targeted approach to understanding the complexities and advancements in IoT and privacy issues over a concise period. The chosen keywords for this review— "Internet of things," "data privacy," "general data protection regulations," and "laws and legislation"—point to a concentrated focus on how IoT technologies intersect with regulatory and privacy concerns, particularly under frameworks such as the General Data Protection Regulation (GDPR). This review exclusively considers articles written in English, which may restrict geographical diversity but aids in maintaining consistency and clarity in the analysis. Overall, this SLR methodology is crafted to provide a thorough examination of recent scholarly articles that discuss critical issues at the intersection of technology, law, and privacy within the rapidly evolving domain of IoT.

Data tool and collection

The data for this study consisted of secondary textual data. On May 06, 2024, information was retrieved from the Scopus academic search engine (https://www.scopus.com). Additionally, advanced search terms were utilized as TITLE-ABS-KEY(Development AND Framework AND Data protection Regulations AND Internet of things) AND PUBYEAR > 2018 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (SUBJAREA,"COMP")) AND (LIMIT-TO (PUBSTAGE, "final")) AND (LIMIT-TO (EXACTKEYWORD, "Internet Of Things") OR LIMIT-TO (EXACTKEYWORD,"General Data Protection Regulations") OR LIMIT-TO (EXACTKEYWORD, "Laws And Legislation") OR LIMIT-TO (EXACTKEYWORD, "Internet Of Things (IoT)") OR LIMIT-TO (EXACTKEYWORD, "Data Privacy")) AND (LIMIT-TO (LANGUAGE, "English")) search terms. The result showed that 8 documents were retrieved.

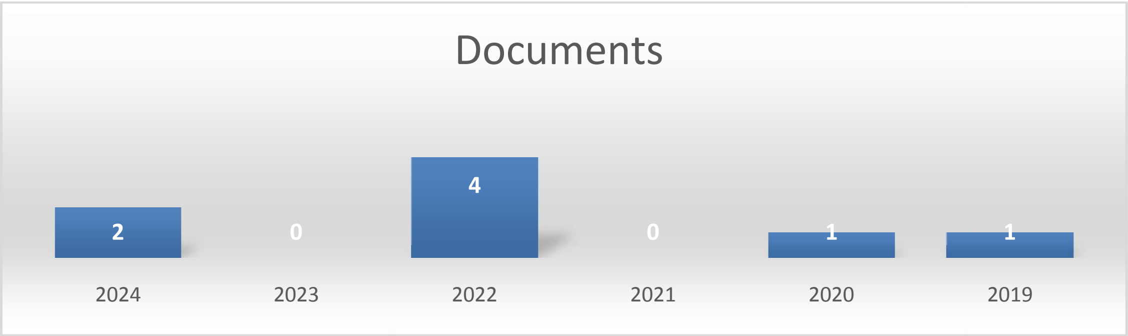
Figure 1: PRISMA Diagram


Identification
screening
Eligibility
Included
The database search: Scopus (Scopus.com 06/May 2024) (n=8)
Records after duplicates are removed. (n= 56)
Records screened (n=8)
Records excluded (n=2)
Full-text articles assessed for eligibility (n=6)
Full-text articles excluded, with reasons (n=2)
Studies included in qualitative assessment (n= 6)
Full articles excluded, with reasons (n=0)
-
Studies included in data extraction (n=6)

IV. RESULT

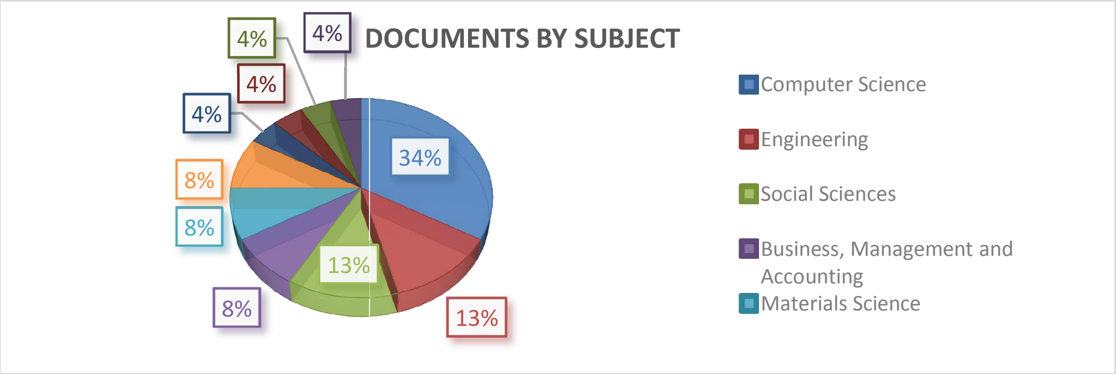
The analysis revealed that while existing security frameworks provide a foundational structure for IoT security, they often fall short in addressing the specific challenges posed by IoT devices and their operational environments. Through the evaluation of advanced security solutions, such as the full stack security architecture and adversarial training models, it was found that these approaches significantly enhance the robustness and effectiveness of IoT security systems. Additionally, the study confirmed the critical need for developers to incorporate privacy considerations at the early stages of IoT device and system design. Regulatory challenges, particularly with GDPR compliance, were identified as a major obstacle, impacting the seamless integration of security measures across IoT platforms. This underscores the importance of continuous adaptation and evolution in security strategies to keep pace with technological advancements and regulatory changes in the IoT landscape.

Figure 1: Document by year



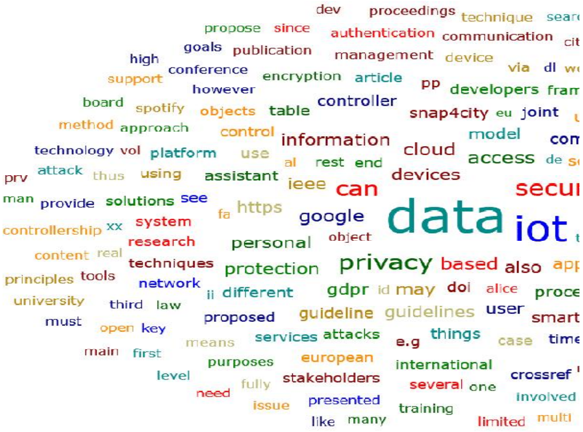
The data outlines the number of documents produced annually from 2019 to 2024. It shows variability in document production over these years, with notable increases and decreases. Specifically, there were 1 document in 2019 and 2020, none in 2021, a peak of 4 documents in 2022, no documents again in 2023, and a partial recovery to 2 documents in 2024. This pattern suggests significant fluctuations that could be attributed to various internal or external factors affecting the production of these documents. The absence of any documents in 2021 and 2023 is particularly striking and raises questions about the reasons behind these gaps—whether they were due to operational pauses, changes in policy, or other influences. The spike in 2022 indicates a temporary surge in activity or interest that waned the following year. It's difficult to draw concrete conclusions without more context on what these documents represent or additional information on influencing factors. However, these fluctuations suggest a dynamic situation where factors influencing document production vary significantly yearly. Understanding these trends would be critical for forecasting future activities and adapting strategies accordingly.

Figure 2: document by subject



The data outlines the distribution of documents across various subject areas, highlighting the differing scholarly or operational output levels in eacMostdocuments, totalling eight, fall under Computer Science, indicating a solid emphasis or active research and development in this field. This is followed by Engineering and Social Sciences, each with three documents, suggesting a moderate activity level in these areas. Business, Management and Accounting, Materials Science, and Mathematics each have two documents showing some engagement but possibly less priority or fewer resources allocated compared to fields with higher outputs. Finally, Chemistry, Economics, Econometrics and Finance, Environmental Science, Physics and Astronomy have the most miniature representations with only one document each, pointing to these areas being less focused upon within the given context. This distribution might reflect the priorities of the institution or entity involved in producing these documents, indicating a strong inclination towards technological and applied sciences with less emphasis on physical sciences and specific areas of social sciences. Understanding why some areas have higher outputs than others could provide insights into strategic focus areas, funding allocation, or trends in research and development within the organization or context from which this data originates.

Figure 3: word cloud



DOI: 10.48175/IJARSCT-18175

The word cloud analysis, with prominent terms like "Data," "IoT," "Privacy," "Internet," "Security," and "Internet of Things," points to a robust focus on the technological and ethical dimensions of the Internet of Things (IoT). The frequent appearance of "IoT" and "Internet of Things" strongly emphasizes this advanced connectivity framework, which integrates physical objects into networked systems via the Internet. The word "Data" is prominently featured to indicatedata management and analytics's crucial role in IoT systems. Alongside these technological terms, "Privacy" and "Security" highlight widespread concern about the challenges and risks associated with data protection and system security in IoT environments. These concerns likely reflect ongoing discussions or research on finding practical solutions to safeguard personal information and secure networked devices against cyber threats. The term "Internet" reiterates the foundational technology enabling IoT, tying all these aspects together into a thematic concentration on how IoT technologies are evolving, how they are managed, and the security and ethical issues they bring to the fore.

V. DISCUSSION

The findings of this study highlight several key aspects of IoT security, particularly in the context of data at rest. One of the primary revelations was the inadequacy of conventional security frameworks when applied to the diverse and technically constrained environment of IoT devices. This inadequacy stresses the necessity for IoT-specific security solutions that are not only effective but also scalable and adaptable to varied IoT applications and infrastructures.

The significance of integrating security measures from the onset of device and system design was evident. The privacy-by-design approach advocated in various studies has proven effective in preempting potential security breaches. However, the real-world implementation of these principles is often hindered by the complexity of IoT ecosystems and the varying degrees of technical expertise among developers. This calls for more streamlined guidelines and tools that can aid developers in implementing these principles more effectively.

Moreover, our evaluation of advanced security methods such as full stack security architectures and adversarial training models showed promising results in enhancing data security. These methods, however, require substantial computational resources and sophisticated implementation strategies, which may not be feasible for all IoT deployments, especially those with stringent resource constraints.

The study also brought to light the complexities involved in adhering to stringent regulations such as GDPR. The regulatory landscape is still evolving, and IoT deployments must remain flexible to accommodate future changes in laws and standards. The tension between technological advancement and regulatory compliance presents a continuous challenge for industry stakeholders.

Ultimately, this discussion underscores the dynamic and multifaceted nature of IoT security. Continuous research and development efforts are crucial to address the emerging security challenges and to ensure that IoT technologies can be trusted and safely integrated into our digital and physical worlds. The collaborative effort between technology developers, regulatory bodies, and security experts will be vital in crafting a secure IoT future.

VI. CONCLUSION

This review emphasizes critical gaps in IoT data security, particularly for data at rest, and suggests that existing frameworks fall short due to their inability to address uniquie challenges in IoT environments. It emphasizes the importance of incorporating privacy-by-design principles from the onset of system design and highlights the need for innovative, resource-efficient security solutions like full stack architectures and adversarial model. Continuous adaptation in response to evolving regulatory landscapes, such as GDPR, is also crucial for integrating effective security measures.

REFERENCES

[1]. Abdulghani, H. A., Nijdam, N. A., Collen, A., & Konstantas, D. (2019). A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective. *Symmetry*, *11*(6), 1–36. https://doi.org/10.3390/sym11060774

[2]. Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. *IEEE Access*, *8*, 23601–23623. https://doi.org/10.1109/ACCESS.2020.2968741

[3]. Kühtreiber, P., Pak, V., & Reinhardt, D. (2022). A survey on solutions to support developers in privacy-preserving IoT development. *Pervasive and Mobile Computing*, *85*, 1–31. https://doi.org/10.1016/j.pmcj.2022.101656

[4]. li Liu, Y., Huang, L., Yan, W., Wang, X., & Zhang, R. (2022). Privacy in AI and the IoT. *Telecommunications Policy*, *46*(7). https://doi.org/10.1016/J.TELPOL.2022.102334

[5]. van Mill, J., & Quintais, J. P. (2022). A Matter of (Joint) control? Virtual assistants and the general data protection regulation. *Computer Law and Security Review*, *45*(May), 105689. https://doi.org/10.1016/j.clsr.2022.105689

[6]. Zhang, P., Wang, Y., Kumar, N., Jiang, C., & Shi, G. (2022). A Security- and Privacy-Preserving Approach Based on Data Disturbance for Collaborative Edge Computing in Social IoT Systems. *IEEE Transactions on Computational Social Systems*, *9*(1), 97–108. https://doi.org/10.1109/TCSS.2021.3092746