Review Article

Applications of the internet of things in library and data privacy

Bal Ram[1],*, Ashish Kumar[2], Surendra Kumar Pal[3]

[1]*Wadia Institute of Himalayan Geology, (D.S.T., Govt. of India), Dehradun, Uttarakhand, India*
[2]*Doon University, Dehradun, Uttarakhand, India*
[3]*Central Library, Tripura, University, Tripura, India*

ABSTRACT

The Internet of Things (IoT) has emerged as a promising technology with trans formative potential in various industries, including libraries. An overview of the applications of IoT in libraries highlights the importance of data privacy considerations in the context of IoT adoption. Libraries are increasingly leveraging IoT to enhance their operations and improve user experiences. Intelligent library management systems, including automated inventory tracking, self-checkout systems, and intelligent shelf management, streamline library processes and optimize resource utilization. Environmental monitoring using IoT sensors ensures the preservation of delicate materials by monitoring temperature, humidity, and air quality in library spaces. IoT-enabled occupancy tracking provides valuable insights into space utilization, enabling effective resource allocation and planning. This paper emphasises the need for libraries to find a balance between harnessing the benefits of IoT technologies and safeguarding patrons' data privacy. By implementing appropriate privacy safeguards, libraries can leverage the potential of IoT to enhance their services while maintaining the trust and privacy of their users.

For reprints contact: reprint@ipinnovative.com

1. Introduction

The application of the Internet of Things (IoT) in data privacy has emerged as a significant area of concern and innovation. As IoT devices become increasingly prevalent in our daily lives, collecting vast amounts of data, and ensuring the privacy and security of that data have become a significant challenge. One key aspect of IoT data privacy is the protection of personal information. IoT devices, such as wearable fitness trackers, intelligent home assistants, or connected cars, gather sensitive data about individuals, including their health information, location data, and daily routines. To safeguard this personal information, IoT applications must implement robust security measures, such as data encryption, user authentication, and access controls.

These measures help prevent unauthorised access or data breaches that could compromise individuals' privacy.[1–6]

The Internet of Things (IoT) has brought about significant advancements in various sectors, and libraries are no exception. The applications of IoT in libraries offer numerous benefits, but it is crucial to consider data privacy implications. IoT enables libraries to streamline operations and enhance user experiences. RFID tags embedded in books facilitate efficient inventory management and automated check-in/check-out processes, saving time for both librarians and patrons. However, proper data privacy measures must be in place to safeguard patron information and ensure the secure handling of data collected from RFID tags. Environmental monitoring using IoT sensors helps protect valuable library materials by guaranteeing optimal conditions for preservation. However, privacy concerns arise if personal data inadvertently gets captured by sensors.

* *Corresponding author.*
  E-mail address: balram@wihg.res.in (B. Ram).

Libraries must anonymise and secure collected data to protect user privacy and comply with data protection regulations.

Occupancy tracking using IoT sensors provides valuable insights into space utilisation, aiding in resource allocation and improving library services. Nevertheless, it is essential to respect user privacy by anonymising tracking data and obtaining proper consent for data collection and processing. Personalised services based on IoT devices, such as wearables or mobile apps, enhance user experiences by offering tailored recommendations, reading lists, and event notifications. Protecting personal data privacy is paramount in these applications, ensuring transparent data handling practices, obtaining user consent, and complying with privacy regulations. IoT-based security systems enhance library safety by monitoring areas and detecting unauthorised access. However, privacy considerations must be addressed to balance security and patron privacy. Surveillance measures should be proportionate, compliant with privacy regulations, and respect the privacy rights of library users.

To ensure data privacy in IoT applications for libraries, privacy-by-design principles should be implemented. Conducting privacy impact assessments, implementing clear privacy policies, and transparently communicating data collection, storage, and usage practices are essential. Libraries must prioritise user consent, data anonymisation, and compliance with relevant privacy regulations to protect patron privacy in the IoT era.[7–10]

2. Literature Review

A literature review provides an overview of the current state of knowledge in a particular field or area of study. It serves as a foundation for further research by identifying gaps in the existing literature or highlighting areas that require more investigation. Additionally, a literature review helps researchers situate their work within the broader scholarly conversation and demonstrate their understanding of the relevant theories and concepts. Pajo and Rauch (2019) provide an insightful analysis of the applications of IoT in libraries and the associated data privacy considerations. It emphasises the need for libraries to balance leveraging the benefits of IoT and safeguarding patron privacy. It is a valuable resource for librarians, researchers, and policymakers interested in understanding the practical implications of IoT adoption in libraries and the measures required to ensure data privacy. Al-Jaafreh and Reyalat (2021) explore the various applications of the Internet of Things (IoT) in libraries and address the critical aspect of data privacy. The review aims to provide an in-depth analysis of IoT applications in library settings and the measures required to ensure data privacy. Al-Fuqaha et. al. (2015) provides a comprehensive survey of the enabling technologies, protocols, and applications within the IoT

landscape. It offers valuable insights into the potential of IoT and its associated challenges, particularly with data privacy and security. This review serves as a foundation for further research and development in the field of IoT.

Kumar and Mittal (2016) provide an overview of the privacy and security challenges associated with the Internet of Things. It emphasises the need for robust security measures, user-centric privacy frameworks, and awareness among users and stakeholders. The review serves as a valuable resource for understanding the privacy and security implications of IoT and offers insights into potential solutions to ensure data protection in IoT systems. Zhang and Li (2018) present a privacy-preserving model based on differential privacy for the IoT. It contributes to the body of knowledge by addressing the need for privacy-enhancing mechanisms in IoT data collection and analysis. The review provides valuable insights into the implementation and potential applications of the proposed model, contributing to the advancement of privacy-preserving techniques in IoT systems. Ram, B., & Karn, B. (2013) the need, use and price of information is increasing daily. And finances the number of resource centres is decreasing, and a new term consortium was born to fill that void. This era is the digital age, where libraries are getting smaller, but richer in information resources. Information is stored, produced and distributed in the form of bits and bytes. Libraries are based on the digitised information of gradually replaced information paper documents. The Internet is essential in making these e-journals available to end users in their resource centres.

Perera, Liu, Jayawardena, and Chen (2017) provide a comprehensive analysis of the Internet of Things (IoT) specifically focused on the industrial market. The authors aim to explore the applications, challenges, and opportunities associated with IoT implementation in the industrial sector. Ram, B., & P., Verma (2023) artificial Intelligence (AI) is the most profound technology we are working on today. Artificial intelligence research focuses on specific goals and the use of certain tools. Research in artificial intelligence includes reasoning, information representation, planning, learning, natural language processing, perception and the ability to move and manipulate objects.[11–15]

Poonia et al. (2018) provide a comprehensive survey of the data privacy and security challenges in IoT-based healthcare systems. It offers valuable insights into the risks, regulations, and potential solutions within the healthcare domain. The review is a valuable resource for healthcare professionals, researchers, and policymakers seeking to understand and address the privacy and security concerns associated with IoT in healthcare. Ram, B., & Singh, K. K. (2020). The library changed from traditional to modern; at that moment, it became an automated library, it became digital and mobile phones worked. Current

cell phones have become an essential part of human life in correspondence, and it also serves the online learning of students. Iorga et al. (2014) provide insights into the challenges and potential solutions for privacy-aware intelligent buildings. The proposed framework offers a comprehensive approach to capturing, communicating, and enforcing privacy policies and preferences. The review serves as a valuable resource for researchers and practitioners in the field of intelligent buildings, contributing to the development of privacy-enhancing mechanisms and practices in IoT-enabled building environments.

Gluhak et al. (2011) focus on providing an overview of the facilities available for conducting experimental research in the IoT domain. The authors aim to highlight the importance of testbeds and experimental platforms in advancing IoT research and development. Kumar, A. et al. (2017) Usually, the advocates in the library are the librarian, subject specialist, lecturers and students in the process of developing the collection, but if we analyse closely, everyone has some disadvantage; it is a fact that a librarian cannot be an expert in all subjects, no matter how experienced he is Experts have biases or prejudices that faculty cannot vouch for all subjects in equal proportion, the student's recommendation cannot guarantee that the desired title will come really used. Ram, B., & Karn, B. (2014) due to information and communication technology, electronic resources are increasingly popular in the scientific community as well as easy to use and also consistent. Electronic resources help online learning functionally increase students' attention and encourage them to be independent learners.

The Internet of Things: A Survey" by Atzori, Iera, and Morabito (2010) provides a comprehensive overview of the Internet of Things (IoT). The authors aim to survey the fundamental concepts, enabling technologies, and applications of IoT. Kumar, A., & Ram, B. (2023) online library services have become increasingly important in today's digital age in catering to users' easy and convenient access to library resources and facilities. Fernández-Caramés and Fraga-Lamas (2018) provide a comprehensive overview of the use of blockchain for the Internet of Things. It covers the technical aspects, potential applications, and challenges of integrating blockchain into IoT systems. The review is a valuable resource for researchers, practitioners, and policymakers interested in exploring the synergies between blockchain and IoT technologies. Ram, B., & Yadav, S. (2022) this study covers several technological and analytical parameters viz distribution of full-length articles per year, classification of works, authors the model of works, degree of cooperation of the author, length of publications, order of authors, etc. Khan et al. (2012) provide an overview of the architecture, applications, and challenges of the Internet of Things in the context of the future Internet. It serves as a valuable resource for

researchers and practitioners interested in understanding the foundational concepts and considerations of the IoT.

3. Applications of the Internet of Things in Library

The Internet of Things (IoT) has revolutionised the library landscape, offering a range of innovative applications that enhance library services and improve operational efficiency. However, the integration of IoT in libraries must also prioritise data privacy to protect patrons' sensitive information. This article explores the applications of IoT in libraries and highlights the importance of data privacy considerations.

1. Smart Library Management: IoT technologies facilitate automated inventory management, enabling real-time tracking of library resources, such as books, CDs, and DVDs. RFID tags and sensors allow libraries to locate items efficiently, automate check-in and check-out processes, and prevent theft. Data privacy measures ensure that patron information is securely stored and accessed only for authorised purposes.
2. Environmental Monitoring: IoT sensors monitor environmental conditions in libraries, such as temperature, humidity, and air quality. This data helps libraries maintain optimal conditions for preserving delicate materials and protecting against damage. Privacy safeguards ensure that the sensors do not inadvertently collect personal information and that data is anonymised and stored securely.
3. Space Utilization and Resource Allocation: IoT-based occupancy tracking systems provide insights into library space utilisation, helping libraries optimise seating arrangements, resource allocation, and facility management. Privacy concerns are addressed by anonymising occupancy data and obtaining user consent when collecting personal information.
4. Personalized Services: IoT enables personalised library experiences by leveraging user data. Beacons and location-based services offer customised recommendations, notifications, and assistance based on patrons' preferences and location within the library. Privacy protections involve obtaining consent for data collection, implementing strict data access controls, and providing transparent information about data handling practices.
5. Security and Surveillance: IoT-based security systems enhance library security by monitoring entrances, exits, and restricted areas. Surveillance cameras and sensors detect unauthorised access, ensuring the safety of patrons and library resources. Data privacy considerations include using encryption for data transmission, restricting access to surveillance footage, and complying with legal regulations.

To safeguard data privacy, libraries should adopt privacy-by-design principles, conduct regular privacy assessments, and comply with data protection regulations such as the General Data Protection Regulation (GDPR). Transparent communication with patrons about data collection, usage, and retention policies is crucial for building trust and ensuring informed consent.

In conclusion, IoT applications in libraries offer numerous benefits, ranging from improved resource management to personalized services. However, data privacy should be a primary concern when implementing IoT solutions in libraries. By prioritizing data privacy and implementing appropriate safeguards, libraries can harness the potential of IoT while respecting patrons' privacy rights and maintaining their trust.

4. Applications of the Internet of Things in Data Privacy

The Internet of Things (IoT) has significant implications for data privacy, as it involves the collection, sharing, and processing of vast amounts of data from connected devices. While IoT offers numerous benefits, it also challenges maintaining data privacy. Here are some applications of IoT in data privacy:

1. Secure Data Transmission: IoT devices can employ encryption protocols and secure communication channels to ensure the confidentiality and integrity of data during transmission. This protects sensitive information from unauthorised access or interception.
2. Privacy-Preserving Data Analytics: IoT data can be processed using privacy-preserving techniques such as differential privacy, which adds noise to the data to protect individual privacy while still enabling meaningful analysis. This allows organisations to derive insights from IoT data without compromising personal privacy.
3. User Consent and Control: IoT applications should prioritise obtaining explicit user consent for data collection, usage, and sharing. Users should have control over the data types collected, the purpose of data usage, and the ability to opt out of data sharing.
4. Anonymization and Pseudonymization: IoT data can be anonymised or pseudonymised to protect the identities of individuals while still allowing for analysis and research purposes. This reduces the risk of re-identification and safeguards individual privacy.
5. Privacy by Design: IoT systems should be designed with privacy considerations in mind from the early stages of development. This includes implementing privacy-enhancing technologies, adhering to privacy regulations, and conducting privacy impact assessments to identify and address potential privacy risks.
6. Data Minimization: IoT applications should follow the principle of data minimisation, collecting only the necessary data for specific purposes. This reduces the risk of privacy breaches and ensures that data collection is proportionate and justifiable.
7. Transparent Data Practices: Organizations deploying IoT systems should communicate transparently with users about data collection practices, storage duration, and data handling policies. Clear and concise privacy policies should be provided to inform users about their rights and how their data will be used.

By incorporating these applications, the IoT can be harnessed while safeguarding data privacy. Organizations and policymakers must collaborate in developing and enforcing privacy regulations that address the unique challenges posed by IoT and ensure that individuals' privacy rights are protected in this increasingly connected world. [15–19]

5. Advantage of the Internet of Things in Libraries and Data Privacy

The Internet of Things (IoT) offers several advantages in the context of libraries and data privacy:

1. Enhanced Library Services: IoT technologies enable libraries to provide more efficient and personalised services to patrons. With IoT devices, libraries can automate processes such as book check-in and check-out, inventory management, and resource tracking. This streamlines operation and improves the overall library experience.
2. Improved Resource Management: IoT sensors and tracking systems allow libraries to monitor the usage and location of books, media, and other resources in real-time. This helps librarians optimise resource allocation, identify popular items, and ensure that materials are readily available to patrons when needed.
3. Data-Driven Decision Making: IoT devices generate vast amounts of data about library operations, usage patterns, and patron preferences. Analysing this data can provide valuable insights for librarians to make informed decisions regarding collection development, space utilisation, and service improvements. Proper data privacy measures ensure that sensitive patron information remains secure and anonymous.
4. Enhanced Accessibility: IoT technologies can improve accessibility for library users. For example, smart devices and beacons can provide location-based assistance to patrons with disabilities, guiding them to access facilities or offering customised recommendations based on their needs.
5. Efficient Space Management: IoT sensors can monitor occupancy levels in different library areas, helping librarians optimise seating arrangements, study spaces,

and resource allocation. This leads to better space management, improved utilisation, and enhanced user experiences.

6. Environmental Monitoring: IoT sensors can monitor environmental factors like temperature, humidity, and air quality in library spaces. This ensures the preservation of delicate materials and creates a comfortable environment for patrons. Data privacy measures ensure that personal information is not collected or linked to environmental monitoring data.

7. Security and Safety: IoT-based security systems, including surveillance cameras and access control systems, can enhance library security. These systems can detect and prevent unauthorised access, ensuring the safety of patrons and protecting library resources. Privacy protections are essential to ensure that surveillance data is securely stored, accessed only by authorised individuals, and compliant with privacy regulations.

While IoT offers numerous advantages in libraries, it is crucial to implement robust data privacy measures. Libraries must prioritise the protection of patron information, obtain consent for data collection and usage, and establish secure data storage and transmission protocols. By integrating IoT technologies with strong data privacy practices, libraries can harness the benefits of IoT while safeguarding patron privacy.

6. Demerits of the Internet of Things in Libraries and Data Privacy

While the Internet of Things (IoT) brings several benefits to libraries, there are also some potential demerits and challenges related to data privacy:

1. Data Security Risks: IoT devices in libraries create additional entry points for potential security breaches. If not properly secured, these devices can be vulnerable to hacking or unauthorised access, leading to the compromise of sensitive patron information and library resources.

2. Data Breaches and Privacy Violations: Inadequate security measures or mishandling of IoT data can result in data breaches or privacy violations. If personal information, borrowing history, or reading habits of library users are exposed or accessed by unauthorised parties, it can lead to privacy concerns and potentially harm individuals' privacy rights.

3. Lack of Standards and Interoperability: IoT devices and systems in libraries often come from different manufacturers and may lack standardised security and privacy protocols. This can create interoperability challenges and make it difficult to ensure consistent and effective data privacy measures across the library's IoT ecosystem.

4. Overcollection of Data: IoT devices can collect vast amounts of data, including personally identifiable information (PII), without a clear purpose or justification. This over-collection of data can increase privacy risks and expose individuals to unnecessary surveillance and profiling.

5. Consent and Transparency Challenges: Obtaining meaningful and informed consent from library patrons for data collection and usage can be challenging. IoT devices may collect data automatically, and patrons may not fully understand the implications or have clear visibility into what data is being collected and how it is being used.

6. Data Ownership and Control: With IoT devices and services in libraries, there is a potential loss of control over personal data for both libraries and patrons. Third-party vendors may collect and store data on behalf of the library, creating concerns about who owns the data and how it is used beyond the library's control.

7. Legal and Regulatory Compliance: Libraries must navigate complex legal and regulatory frameworks when it comes to data privacy, such as the General Data Protection Regulation (GDPR) or local privacy laws. Ensuring compliance with these regulations while implementing IoT technologies can be challenging, particularly if libraries lack the necessary resources and expertise.

To address these demerits, libraries must prioritize data privacy and security in their IoT implementations. They should conduct privacy impact assessments, adopt privacy-by-design principles, implement robust security measures, and provide transparent communication to patrons about data collection and usage practices. Collaboration with privacy experts and adherence to relevant regulations is crucial to mitigate the demerits associated with IoT in libraries and safeguard data privacy.

7. Conclusion

In conclusion, the applications of the Internet of Things (IoT) in libraries have the potential to enhance library services and operations greatly. IoT technologies can automate processes, improve resource management, and enable data-driven decision-making. However, it is crucial to prioritise data privacy and security in implementing IoT in libraries. Libraries must adopt robust data privacy measures, including secure data transmission, user consent and control, anonymisation, and privacy by design principles. By effectively addressing data privacy concerns, libraries can harness the benefits of IoT while ensuring the protection of patron information and maintaining trust in the library ecosystem.

8. Source of Funding

None.

9. Conflict of Interest

None.

References

1. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*. 2015;17(4):2347–76.
2. Al-Jaafreh A, Reyalat M. Internet of Things (IoT) Applications in Libraries: A Systematic Review. *J Inf Sci Theory Pract*. 2021;9(1):67–88.
3. Atzori L, Iera A, Morabito G. The Internet of Things: A survey. *Computer Networks*. 2010;54(15):2787–805.
4. Fernández-Caramés TM, Lamas PF. A review on the use of blockchain for the Internet of Things. *IEEE Access*. 2018;6:32979–3001.
5. Gluhak A, Krco S, Nati M, Pfisterer D, Mitton N, Razafindralambo T. A survey on facilities for experimental internet of things research. *IEEE Communications Magazine*. 2011;49(11):58–67.
6. Iorga M, Koushanfar F, Saxena N. Towards privacy-aware smart buildings: Capturing, communicating, and enforcing privacy policies and preferences. *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2014;p. 67–78.
7. Khan R, Khan SU, Zaheer R, Khan S. Future internet: The Internet of Things architecture, possible applications and key challenges; 2012. p. 257–60.
8. Kumar A, Ram B. Application and Significance of Web-Based Library Services. *Int Res J Modernization Eng Technol Sci*. 2020;5(05):3397–400.
9. Kumar A, Kumar R, Pandey SK. Analysis of the Collection Development Policies: A Case Study of the Libraries of Kumaun University. *Int J Inf Manag*. 2017;2(5):54–9.
10. Kumar N, Mittal P. A review on Internet of Things (IoT) in the perspective of Privacy and Security. *Int J Comp Appl*. 2016;140(11):10–3.
11. Pajo A, Rauch S. The Internet of Things in Libraries: A Systematic Literature Review. *Library Hi Tech*. 2019;37(3):441–58.
12. Perera C, Liu CH, Jayawardena S, Chen M. A survey on Internet of Things from industrial market perspective. *IEEE Access*. 2017;5:5472–82.
13. Poonia RC, Sharma S, Kumar V. Data privacy and security challenges in IoT-based healthcare systems: A comprehensive survey. *J Network Comp Appl*. 2018;103:1–17.
14. Ram B, Karn B. Impact of UGC InfoNet Consortia on the users of universities of Jharkhand in Eastern India. *Int J Sci Eng Technol Res (IJSETR)*. 2013;2(4):823–32.
15. Ram B, Karn B. Study of UGC Infonet E-Resources Consortia in Universities of Eastern India. *Int J Comput Sci Inf Technol*. 2014;5(6):977–983.
16. Ram B, Verma P. Artificial intelligence AI-based Chatbot study of ChatGPT, Google AI Bard and Baidu AI. *World J Adv Eng Technol Sci*. 2023;8(01):258–61.
17. Ram B, Singh KK. Innovative library services in mobile technology: A recent approach. *Int J Inf Dissemination Technol*. 2020;10(4):192–4.
18. Ram B, Yadav S. Bibliometric Study of DESIDOC Journal of Library and Information Technology from 1981-2018. *Libr PhilosophyPract*. 2022;p. 1–13.
19. Zhang X, Li X. IoT data privacy-preserving model based on differential privacy. *Wireless Networks*. 2018;24(5):1377–87.

Author biography

Bal Ram, Librarian

Ashish Kumar, Librarian

Surendra Kumar Pal, Assistant Librarian