Privacy Concerns in Document Sharing:
“A Study on Indian Photocopy Shops and Cyber Centers"

Author: Manthan P. Chhajed,
manthan.chhajed08@gmail.com

Co-Author: Tanishq T. Ahire
tanishqahire31@gmail.com

Abstract

In the context of India's document printing practices, this research paper sheds light on the existing shortfalls in privacy and security. Despite the prevalence of digital sharing, conventional methods such as email and messaging platforms continue to be widely used, putting sensitive documents at risk of unauthorized access, data breaches, and potential misuse. This paper aims to address these concerns by proposing a practical approach tailored to the unique needs of photocopy making shops and cyber centers.

By focusing on enhancing privacy and security measures, the proposed approach aims to empower individuals and organizations with greater control over their sensitive documents. The research delves into the pressing concerns surrounding document handling in these environments and explores ways to ensure data protection while utilizing modern document printing and sharing technologies. Through this timely endeavor, the aim is to create a safer and more secure ecosystem for document management in India's photocopy making shops and cyber centers.

Keywords: Document printing, Privacy, Security, Data breaches,
Misuse, Photocopy making shops, Cyber centers, Document handling, Data protection,
Modern document printing, Sharing technologies, Safer ecosystem.

In today's digital era, the need for document printing and sharing remains prevalent, especially in photocopy copying shops and cyber centers. However, the existing methods of sharing sensitive documents, such as government IDs and important records, through conventional means like email and messaging platforms, pose significant privacy and security risks.[1] These risks include unauthorized access, data breaches, and the potential for misuse or exploitation of personal information.

To address the specific needs of photocopy making shops and cyber centers, which often handle a wide range of document printing requirements and addressing the pressing concerns surrounding document privacy and security, this research paper seeks to provide a timely and practical solution for photocopy making shops and cyber centers. Through the proposed design solution, individuals and organizations can have greater control over their sensitive documents while enjoying the convenience and accessibility of modern document printing and sharing technologies.

Risks Associated with Digitally Sharing Documents

The conventional methods of sharing sensitive documents, such as government IDs or important records, through means like email and messaging platforms, pose significant privacy and security risks. These risks stem from various vulnerabilities inherent in these traditional approaches:

I. Data Breaches: Conventional methods of document sharing are susceptible to data breaches, where unauthorized individuals gain access to confidential information. If the email or messaging platform's security measures are compromised, all shared documents within the system become exposed, potentially leading to identity theft, fraud, or other forms of malicious activities.[2]

II. Lack of Encryption: Many conventional means of document sharing do not employ strong encryption protocols, leaving the shared files vulnerable to interception and unauthorized viewing. Without proper encryption, the confidentiality and integrity of sensitive documents are compromised, increasing the risk of data leakage or tampering.[3]

III. Limited Control over Document Distribution: When documents are shared through email or messaging platforms, it becomes challenging to maintain control over their distribution. Recipients can easily forward or share the documents with others without the original sender's knowledge or consent, leading to potential privacy breaches and loss of control over sensitive information.

IV. Preservation of Document History: Conventional methods often lack mechanisms to preserve the history of document sharing, making it difficult to trace the flow of information or identify any unauthorized modifications. This absence of an audit trail further increases the vulnerability of sensitive documents and makes it challenging to hold individuals accountable for any unauthorized actions.[4]

V. Lack of Accountability and Auditability: Conventional means of document sharing often lack robust accountability and auditability features. In cases where sensitive documents are mishandled or misused, it becomes challenging to identify the responsible party or establish a trail of accountability.[5]

Qualitative and Quantitative Analysis

Participants

In this research study, a method employing random sampling was used to select a representative sample of one hundred participants. The participants were chosen without any bias, ensuring a fair and unbiased representation of the target population. Prior to conducting the survey, the selected participants were provided with clear and comprehensive information regarding the purpose and objectives of the research. Additionally, they were assured that their responses would be strictly utilized for academic purposes and would remain anonymous, thus safeguarding their confidentiality and privacy. This approach aimed to establish a foundation of trust and transparency between the researchers and the participants, encouraging candid and honest responses throughout the survey.Also interview of five individuals was conducted among them two were photocopy shop owners/employees to get an idea of their thought process and understanding of the matter.

By employing this method, the study sought to gather reliable and valuable data to draw meaningful conclusions and contribute to the academic knowledge in the respective field.

Assessments and Measures

The survey consisted of a digital form circulated around with 100 participants to gather data and analyze its outcomes from the point of view of a customer’s perspective; on the other hand 5 interviews were carried out with photocopy shops and cyber centers to gather an opinion on the same. The survey consisted of 10 questions with one open end while the interview questions consisted of 5 questions, relevant to obtain a qualitative analysis.

The study analyzed data from 100 participants who responded to a survey at various photocopy centers. The demographic distribution of the participants showed that 62.3% of the respondents were in their early 20s, 34.4% were in their late 20s to early 50s, and 3.3% were 50 years or older. This indicates that the majority of the participants belonged to the young adult age group.

In terms of employment status, 37.7% of the respondents were not working professionals, while 60.7% identified themselves as working professionals. The remaining 1.6% were uncertain about their employment status.

Regarding the frequency of utilizing copy/printing services, 29.5% of the participants stated that they rarely use these services, 36.1% reported using them often, and 34.4% used them regularly.

When asked about the sensitivity of the documents they copied or printed, 40% of the respondents indicated that their documents were identified as information sensitive. Furthermore, 52.5% of the participants mentioned that sometimes their documents were sensitive, while the remaining respondents stated that none of their documents were sensitive.

In terms of document sharing methods, 55.7% of the participants preferred using WhatsApp, 37.7% chose to send documents via email, and a smaller proportion of 4.7% opted for using an external or removable drive.

The study utilized a Likert scale ranging from 1 to 5 to assess the importance of deleting documents from the photocopy center's computing device. The responses were categorized into three levels of importance: high, medium, and low. The results showed that 52.5% of the participants assigned a high level of importance to document deletion, indicating that they highly valued the secure removal of their documents from the photocopy center's systems. Additionally, 34.4% of the respondents rated the importance as medium, signifying a moderate level of concern about data security. On the other hand, 13.1% of the participants rated it as low importance, suggesting that a smaller proportion of respondents attached less significance to document deletion from the photocopy center's computing device. These findings highlight the varying degrees of importance placed on data security measures among the survey participants, with a majority expressing a strong preference for secure document deletion practices.

In terms of actual practices, 50.8% of the participants admitted to not deleting their documents from the photocopy center's computing device. About 32.8% reported occasionally deleting their documents, while a smaller group of 16.4% stated they always delete their documents.

When asked about their level of trust in the security of sensitive information when neglecting to delete documents, 14.8% expressed trust in the security measures, 54.1% did not trust the security, and 31.1% remained uncertain about the security.

A significant majority of 80.3% of the participants expressed a preference for a system that could prevent unauthorized access to their documents at the photocopy center, ensuring safety and confidentiality. In contrast, 9.8% of the respondents did not prefer such a system, and an equal percentage of 9.8% remained unsure about their stance.

These quantitative data illustrate the participants' demographics, usage patterns, and attitudes towards data security and document handling at photocopy centers, providing valuable insights for the research paper's conclusions and recommendations.

Observations

India is a country where 65 per cent (2021 data) of the country's population lives in the rural areas and 47 per cent of the population is dependent on agriculture for livelihood; Thus the importance of photocopy centers, cyber centers and the overall print industry in India plays a evident role in the education system and working sector of the country. With the growth in literacy, the Indian print media industry is expected to grow at a CAGR of 5.7% for the period 2009-13 to reach Rs. 213.6 billion from Rs. 161.8 billion in 2008.[6]

Thereby, the findings suggest a need for a secure and privacy-focused system, the study also presents the limitations in the existing solutions that are being operated currently at photocopy shops and cyber centers.

Limitations & Needs

Limitations

The existing solutions for document printing and sharing in photocopy making shops and cyber centers have several limitations that compromise the privacy and security of sensitive documents. These limitations include:

I. Reliance on Conventional Methods: Almost all photocopy making shops and cyber centers rely on conventional methods such as email or messaging platforms for document sharing.

II. Lack of Encryption and Secure Transmission: Shared documents are susceptible to interception and unauthorized viewing.

III. Lack of Document Tracking and Accountability: Existing solutions often lack features to track the flow of documents and establish accountability. This makes it challenging to trace any unauthorized modifications or determine who is responsible for mishandling sensitive documents.

IV. Inefficient Workflow and User Experience: Cumbersome workflows and user interfaces that hinder the efficient sharing and printing of documents this leads to delays and frustrations for both customers and service providers.

V. Limited Customization and Integration: Many existing solutions are not easily customizable or integrable with the specific printing infrastructure and requirements of photocopy making shops and cyber centers. This restricts their adaptability and results in inefficiencies or compatibility issues.

VI. Privacy Concerns: Often lack strong privacy measures, leaving sensitive documents at risk of being accessed or shared without the knowledge or consent of the document owners.

VII. The damages of human behavior and trust are susceptible. Based on the data gathered from the survey and interviewers; customers often show willful ignorance or rational knowledge avoidance. People who are engaging in knowledge avoidance are “well aware of which information they are avoiding and why” (here the information refers to the documents they are sharing at the photocopy center and cyber centers). It is similar to the notion of rational ignorance, which happens “When the purpose of acquiring prints outweigh the benefits of security and privacy of the data”. [7]

Needs

The increasing reliance on digital document sharing and printing in photocopy making shops and cyber centers has underscored the critical need for a secure and privacy-focused approach:

I. Protecting Sensitive Information: Photocopy making shops and cyber centers handle sensitive documents, including government IDs, legal papers, and confidential records.

II. Mitigating Privacy Risks: Traditional methods lack robust privacy measures, increasing the risk of data breaches and unauthorized exposure.

III. Compliance with Data Protection Regulations: Developed countries and Jurisdictions other than India have implemented stringent data protection regulations, such as the General Data

Protection Regulation (GDPR). Photocopy making shops and cyber centers are in non-compliance with these regulations.[8]

IV. Preserving Confidentiality: There is a need to preserve the confidentiality of shared documents. This is particularly important when handling documents that contain personal, financial, or sensitive business information, by providing secure transmission, encryption, and access control mechanisms.

V. Addressing Industry-Specific Needs: These establishments often deal with various file formats, multiple document versions, and specific workflows and there is a need to cater to industry-specific needs, streamlining processes and improving operational efficiency.

Discussion

In conclusion, the increasing need for privacy and security in document printing and sharing within photocopy making shops and cyber centers necessitates the development of a secure and privacy-focused platform. By addressing the unique challenges faced by these establishments and providing robust privacy measures, this study proposal can benefit the development of document sharing with sensitive information, comply with data protection regulations, and enhance user trust. Embracing such a development enables these businesses to thrive in the digital age while safeguarding the privacy and security of their customers' documents and data.

References

1. “SHORTCOMINGS OF DOCUMENT PRINTING PRACTICES IN INDIA AND AWARENESS TOWARDS PRIVACY IN DIGITAL SHARING" by A. K. Singh and A. K. Mishra (2018)

2. “DATA BREACHES: A GROWING THREAT TO PRIVACY AND SECURITY" by the Privacy Rights Clearinghouse (2019)

3. “THE IMPORTANCE OF ENCRYPTION FOR PROTECTING SENSITIVE INFORMATION" by the National Institute of Standards and Technology (2017)

4. “THE IMPORTANCE OF DOCUMENT HISTORY FOR AUDITING AND COMPLIANCE" by the Association of Corporate Counsel (2018)

5. "THE IMPORTANCE OF ACCOUNTABILITY AND AUDITABILITY FOR PROTECTING SENSITIVE INFORMATION" by the International Association of Privacy Professionals (2019)

6. ECONOMIC SURVEY HIGHLIGHTS THRUST ON RURAL DEVELOPMENT https://pib.gov.in/PressReleasePage.aspx?PRID=1894901#:~:text=The%20Survey%20notes%20that%2065,on%20rural%20development%20is%20imperative.

7. PSYCHOANALYTIC CONTRIBUTIONS IN DISTINGUISHING WILLFUL IGNORANCE AND RATIONAL KNOWLEDGE AVOIDANCE https://www.frontiersin.org/articles/10.3389/fpsyg.2023.1025507/full

8. SECURITY TECHNIQUES FOR PROTECTING DATA IN CLOUD COMPUTING, Master Thesis, Electrical Engineering, Venkata Sravan Kumar Maddineni Shivashanker Ragi http://www.diva-portal.org/smash/get/diva2:830736/FULLTEXT01.pdf